CROSS-BORDER SURVEILLANCE AND THE RIGHT TO PRIVACY: LEGAL REMEDIES IN THE AGE OF 5G AND IOT

Syed Shaharyar Ahmed[*]

Abstract

The advent of cross-border surveillance in the digital realm poses new challenges to the right to privacy, particularly with the introduction of 5G networks and the Internet of Things (IoT). These developments offer unprecedented global interconnectedness and innovation but also provide new opportunities for large-scale data retention and transnational flows of information and increase the likelihood of surveillance by states and corporations that transcend traditional jurisdictional boundaries. This paper examines the conflict between cross-border surveillance and the international human rights norm of privacy, particularly the European Convention on Human Rights, the International Covenant on Civil and Political Rights and emerging soft law. It assesses the effectiveness of the legal, judicial, and data protection, and cross-border collaboration frameworks, in addressing violations of the privacy right in a hyper-connected world. Through the analysis of fragmented and disjointed legal and regulatory frameworks for state surveillance, this paper underscores the mismatch between the law and contemporary technological realities. It seeks the establishment of coherent global frameworks and international legal instruments to solve this problem. This paper advocates for the creation of streamlined global frameworks and international legal instruments for resolving these issues.

Keywords: Digital Surveillance, Cross-Border Surveillance, Privacy, Mass Surveillance.

Introduction

The process of conducting surveillance involves the gathering of data concerning a person, group of persons, places or entities through close and continuous observation. The basic objectives of conducting surveillance include crime detection or prevention, and intelligence gathering.

[*]Syed Shaharyar Ahmed is an LLM scholar studying International Technology Law at Vrije Universiteit Amsterdam, Netherlands. He is a litigation attorney and partner at Ibrar & Associates Law Firm, Lahore. ORCID ID: https://orcid.org/0000-0003-0663-4680.

Proximity-based observations, electronic surveillance and data collection are the major modes of conducting surveillance. While surveillance transcends boundaries of a particular state and spreads over a cluster of states, it takes the form of what is referred to as "Cross-border Surveillance".[1] This concept is not new; however, it has gained prominence in recent years due to its manifestation and how it is negatively affecting the right to privacy. The right to privacy in general, and digital privacy in particular, gets compromised when a state or non-state actor conducts surveillance. This paper will focus on the right to digital privacy more, as cross-border surveillance directly impacts digital privacy.[2]

Digital privacy fundamentally means that an online user's interaction over the internet and electronic media is protected from unwanted interference. For instance, a person's social media messages, website browsing and other details shouldn't be monitored as it would be tantamount to invading his/her privacy. The emergence of technologies such as generative AI, 5G and IoT has drastically increased the risks associated with digital privacy, as these advancements have made cross-border surveillance much easier and stealthier.[3] The integration of 5G networks and Internet of Things (IoT) technologies has revolutionised the global cyberspace by allowing rapid data transfers, low-latency communication, and immersive interoperability of devices. This generation leap in technology has led to the amplification of cross-border surveillance capabilities, which can severely impact the right to privacy of individuals.[4]

The 5G/IoT-led cross-border surveillance system can be deployed by state and non-state actors, and through network slicing, edge computing or ubiquitous sensors, they can penetrate and conduct cross-border surveillance. These actions would lead to a breach of traditional legal safeguards, creating jurisdictional defects and regulatory gaps. 5G and IoT allow for granular user tracking through unique identifiers (e.g., IMSI), which exposes individuals to identity-based surveillance.[5] This further worsens when IoT devices exacerbate this risk by collecting real-time biometric and behavioural data. This research paper will build upon the core concepts elaborated above using research methodologies such as comparative, analytical, doctrinal and descriptive approaches.

Various existing legal frameworks will be discussed with references to landmark case laws on this subject matter.[6]

Existing Legal Frameworks Governing Digital Privacy

While there is no existing international legal framework which provides safeguards against cross-border surveillance, there are specific legal instruments that advocate for the protection of digital privacy. For instance, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) 1966, provides that *"no one shall be subjected to arbitrary or unlawful interference with* ***his privacy****, family, home* ***or correspondence****"*. The phrases such as privacy and correspondence have been interpreted to include protection against surveillance. The same was clarified by the general comments no. 16 & 37 of the UN Human Rights Committee that mass-surveillance, if used disproportionately and indiscriminately, can violate Article 17 of ICCPR.[7] Similarly, Article 12 of the Universal Declaration on Human Rights (UDHR) provides that *"no one shall be subjected to arbitrary interference with his privacy…."* Even though UDHR is not legally binding, it has obtained the status of customary international law and is therefore used as a fundamental standard in many national legislations.[8]

The European states are leading the globe in data privacy and protection laws. For instance, Article 8 of the European Convention on Human Rights (ECHR) provides safeguards against privacy, family life and correspondence of a person. The same was upheld by the ECtHR in cases of Liberty v. UK and Big Brother Watch v. UK. Similarly, Article 3 of the EU General Data Protection Regulation (GDPR) 2018 has restricted cross-border data transfers to countries without proper safeguards.[9] The Article mandates data processing safeguards and requires legal grounds to be explicitly stated if personal data of any user is being requested by a foreign state/authority. It requires mechanisms such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCR) for lawful data transfers.[10] The GDPR has played a significant role in curbing cross-border surveillance by state actors, as seen in the Schrems I & II judgments. Convention 108+ (also referred to as the Modernised Convention for Protection of Individuals with regard to the Processing of Personal Data) is a treaty between EU member states that focuses on data privacy and data protection.

Article 14 of this treaty requires the parties to ensure adequate data protection safeguards for cross-border data transfers.[11] Similarly, the United Nations General Assembly (UNGA) Resolution 68/167(2013) [12] and Resolution 73/179 (2018) [13] affirmed that privacy protection is essential against modern surveillance and recognised that cross-border surveillance poses a serious threat to the right to privacy, and urged all states to adhere to their obligations in this regard.

Globally, the most powerful privacy law continues to be the GDPR. It has established principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, and rights for data subjects (access, rectify, erase, or port information). The EU's regulatory reach in the digital sphere also includes DORA – Digital Operational Resilience Act for the Financial Sector, and the EU AI Act, which governs artificial intelligence through a risk-based framework, including bans on manipulative uses of AI and biometric surveillance. [14] There are also governance issues regarding transnational data flows that the EU has with other nations, which require an adequacy decision or protective measures like Standard Contractual Clauses. There's also the Digital Personal Data Protection Act (DPDPA), a modern take on privacy frameworks that goes into effect July 2025, which centres around consent with an emphasis on minimal retention periods. Fiduciary responsibilities will incur breaching obligations with steep penalties for failure.[15]

Australia and other countries like China and Malaysia have strengthened privacy laws with the introduction of children's privacy codes, age restrictions on social media use, and tighter regulations on data security, as well as cross-border data transfers. This reflects a global trend towards stricter data governance. It can be said that there is still a legal gap concerning digital privacy frameworks in Australia, as these reforms only recently came into effect, while showing an effort to protect personal information, particularly noting that these laws are increasingly becoming multilayered and elaborate.[16]

Additionally, businesses, as well as individuals, must legally comply with various evolving regulations which often conflict due to advancing technology which moves faster than regulation frameworks, leaving no room for outdated concepts regarding jurisdiction to too rigid notions of where or what constitutes a borderless zone concerning surveillance amidst competing business interests, revealing whole intertwined cul-de-sacs.[17]

Landmark Cases Governing Cross-Border Surveillance and Right to Privacy

The jurisprudence regarding cross-border surveillance and the right to privacy has developed through various case decisions made primarily by European Courts. Some of these landmark cases and their impact on reinforcing the right to digital privacy are provided as follows:

1. *Schrems I (2015)*

In 2015, an Austrian Privacy Advocate, Mr Maxmillian Schrems, lodged a complaint against Facebook Ireland. He challenged the legality of the Safe Harbour Agreement between the US and EU, through which data transfers were made to the US. As per this agreement, the US had access to data transfers of users without adequate safeguards, and hence, EU citizens' data was compromised. The Court of Justice of the European Union (CJEU) was of the view that the Safe Harbour Agreement allowed US Intelligence Agencies diverse access to EU citizens' data, which was disproportionate and unwarranted by EU Law. Consequently, the CJEU declared the Safe Harbour Agreement invalid, finding it against the right to privacy of EU citizens.[18] This jurisprudential development was of the first of its kind, as it led to data privacy protection against cross-border/mass surveillance conducted by intelligence agencies of foreign states like the US.

2. *Schrems II (2020)*

After the invalidation of the Safe Harbour Agreement, the EU-US Privacy Shield was established to provide for a new framework governing data transfer. Schrems also challenged this new framework on similar grounds adopted in the previous case, that it lacked adequate safeguards for the right to privacy of EU citizens. The CJEU observed that under Section 702 of the Foreign Intelligence Surveillance Act (FISA), the US intelligence agencies had access to the EU citizens' personal data.

The Court stressed that Data Transfers Impact Assessments (DTIA) must be conducted before transferring data to third countries. Furthermore, the Court ruled that a thorough assessment of the laws of third countries should be done so that EU Citizens' data is adequately protected. Ultimately, the Court declared the EU-US Privacy Shield framework invalid as well since it lacked adequate protection for the right to privacy of EU Citizens.[19]

3. *Big Brother Watch v. UK*

In the case of Big Brother Watch v. UK, the matter before the European Court of Human Rights (ECtHR) was concerning the UK's mass surveillance regime. The UK has a mass surveillance program which allows it to obtain a vast amount of personal data without users' consent, including metadata information as well. The Court held that the UK's mass surveillance regime violated the right to privacy as it lacked adequate safeguards. The Court was of the view that in extraordinary circumstances, surveillance could be conducted for which reasonable suspicion and strict necessity are fundamental pre-requisites. Unchecked use of mass surveillance amounts to a violation of Article 8 of the ECHR. [20]

4. *Puttaswamy v. Union of India*

Justice K.S. Puttaswamy (a retired High Court Judge) filed a petition in 2012, which challenged the constitutional validity of the "Aadhaar Program", wherein the biometric identification was required for collecting the private data of persons (including fingerprints and iris scans) for obtaining welfare perks. The government defended their Aadhar program because privacy is not a fundamental right, and they relied on the 1954 M.P. Sharma and 1962 Kharak Singh ruling, in which warrantless search under the colonial-era legal framework and invasive police surveillance were declared to be constitutional. The Court overturned the colonial-era judicial precedents and revamped the concept of privacy. The Court elaborated that privacy is a cornerstone of human autonomy, dignity and informational self-determination. The right to privacy was declared as a fundamental human right under Articles 14, 19 and 21 of the Indian Constitution. This landmark ruling led to the development of India's first comprehensive data protection legal framework – the Digital Personal Data Protection Act (DPDPA) 2023.

Under this Act, the user's consent was made mandatory for data collection, the data breaches were penalised with fines as much as 250 crore Indian Rupees, and a Data Protection Board (DPD) was also established for governing enforcement mechanisms. This judgment reshaped the concept of digital rights in an era which is governed by artificial intelligence, cross-border surveillance and algorithmic dominance.[21]

Impact of 5G and IoT on Cross-Border Surveillance

Furthermore, the advancement in technology and the advent of 5G and IoT have further complicated the phenomenon of cross-border surveillance. The integration of 5G and the IoT has enhanced surveillance capabilities by allowing rapid, more reliable and widespread connectivity for a plethora of devices and applications. This combination provides for real-time monitoring in smart cities and other applications.[22] 5G's rapid speed and minimal latency times allow for real-time data transfer between various IoT devices, such as digital sensors, CCTV cameras, and other surveillance equipment, enabling advanced surveillance capabilities. The concept of smart cities has been made possible due to 5G-enabled IoT devices through which surveillance of an entire city can be done remotely, which includes supervising traffic flow, environmental conditions and public safety. States conducting cross-border surveillance have therefore access to these facilities due to the 5G and IoT-enabled networks.[23] Surveillance networks working on 5G models are more secure against potential data breaches and unauthorised access due to advanced encryption and authentication models used in 5G's enhanced networking capabilities. Furthermore, 5G has enabled remote surveillance of critical infrastructure and industrial processes, which has allowed for timely intervention for the prevention of potential threats. Mostly used applications of 5G and IoT networking include video surveillance, connected vehicles, remote healthcare monitoring systems, and smart grid systems to control and monitor power grids.[24]

While the deployment of 5G and IoT has led to a generational advancement in conducting mass/cross-border surveillance, it has equally raised potential concerns and threats to the right to privacy and the security of persons. The interconnected IoT devices usually generate a massive amount of data, which contains information about the privacy of individuals owning and utilising such devices at homes and offices, and the potential misuse of which could result in a serious breach of users' data privacy.[25]

Furthermore, the complicated nature of 5G and IoT interconnectivity makes them prone to cyber-attacks and data breaches, either from within or outside the ecosystem. The use of 5G and IoT for conducting cross-border surveillance raises severe ethical concerns about personal freedom, right to privacy and security, as well as the algorithmic biases suffered by surveillance networks.[26]

Challenges in Regulating Cross-Border Surveillance

Data privacy, cross-border data collection and sovereignty regulation are primary constraints when it comes to cross-border surveillance. Each region has its own legislative framework governing data transfers, for instance, the GDPR in Europe, PIPL in China and LGPD in Brazil have rigid rules for data collection, processing and sharing. Conducting cross-border surveillance is easy in states where there are flexible and weak data governance regulations, such as in third-world countries like Bangladesh, Nepal and Afghanistan. States often use Standard Contractual Clauses (SCCs) for deciding data collection, access, residency and transfer protocols.[27] Sometimes, states may request special access to users' data through these SCCs for conducting cross-border surveillance. Although SCCs offer legal predictability, their practical consequences depend on factors such as judicial process, regulatory oversight, and willingness to implement requisite safeguards. The objective of conducting cross-border surveillance is equally relevant; health agencies actively use cross-border surveillance for supervising the pandemic situation, as was the case during the COVID-19 pandemic.[28]

Regulation of cross-border surveillance is often handicapped by obstacles emerging from jurisdictional conflicts, technological complexity, and differing legal frameworks. These challenges undermine the right to privacy in the era of 5G and IoT, where the data transfers transcend borders. Surveillance laws vary drastically among different states. For instance, as per the GDPR, judicial oversight is required to obtain access to data within the EU. In contrast, China's National Intelligence Law obligates companies to assist with state surveillance. Similarly, the difference in data localisation laws equally impacts the cross-border surveillance.[29] For instance, countries like India and Russia stress maintaining data locally, which allows them to conduct domestic surveillance, while it hinders global compliance efficiently.

Extra-territorial conflicts are another challenge. For instance, the U.S. CLOUD Act allows the authorities to request cross-border data access, which is in stark opposition to the restrictions imposed by the GDPR. Moreover, the Mutual Legal Assistance Treaties (MLAT), not being updated with the developments in technology, are resulting in delays even in cases of lawful data access.[30]

Even though 5G and IoT connectivity promise improved cross-border surveillance, the technological vulnerabilities they possess are equally concerning. Decentralised IoT devices don't have uniform standards for security, which allows for entry points for potential data breaches. Metadata collection is not regulated correctly, which allows for indirect surveillance.[31] Some nations prioritise national security more than privacy, such as the U.S. FISA Section 702, which allows for warrantless surveillance of non-US citizens, which is against the EU legal framework governing human rights. The definition of "legitimate surveillance" is not uniform, which hinders the practical applicability of international legal instruments. There is no accountability mechanism for tackling cross-border surveillance. The Data Protection Authorities (DPA) don't have sufficient funding for cross-border enforcement. Similarly, there is no global body that could audit cross-border surveillance programs, which leads to severe accountability gaps in surveillance.[32]

Emerging threats include the use of cross-border surveillance under the guise of state-sponsored exploitation. The governments can exploit IoT devices (e.g., smart city sensors) for conducting surveillance under the excuse of national security. Similarly, compromised 5G hardware can lead to covert data access. There are no legal frameworks that address real-time biometric tracking via IoT devices. Furthermore, with the emergence of AI, AI-driven surveillance networking would outpace existing legal frameworks, and hence, no legal action could be taken to curb such breaches of data privacy.[33]

Legal Remedies and Regulatory Approaches

Legal remedies and regulatory approaches to tackle cross-border surveillance are evolving but remain confusing and often inefficient against the robust state intelligence infrastructures. There is a need to develop a uniform legal framework in the form of a multilateral treaty mutually agreed upon by the states governing cross-border surveillance.

Furthermore, existing mutual legal assistance treaties must be modernised to address the technological advancements made through 5G and IoT networking.[34] AI-driven compliance tools can also be deployed for real-time monitoring of data access and transfers. It is crucially important to strengthen international cooperation, improve transparency, and have binding international legal frameworks, which are crucial for ensuring that the right to privacy is duly protected in the digital age of 5G and IoT. The future of privacy protection relies not only on prospective legal instruments but also on the political will of states to curb their own surveillance potential and respect individuals' privacy across borders.[35]

The privacy rights infringements mentioned above could be better protected through the legal and regulatory suggestions provided below, focusing specifically on surveillance across borders: -

1. A clear guideline on the compliance principles of proportionality, necessity, legality, and transparency within state surveillance activities is still lacking. An enforcement-specific document directly addressing these gaps, containing minimum requirements for surveillance activities, is necessary because general human rights treaties, such as ICCPR, lack sufficient specificity. Soft law instruments also serve no purpose in this matter as they are abstract and vague without definition or description.[36]

2. Develop distinct policies that allow citizens to legally appeal unlawful surveillance targeting them or even non-citizens through independent judicial bodies governing cross-border surveillance programs. Many foreign nationals face great injustice, as most of these monitoring systems function behind closed doors with no prerequisite legal judgment backing them.[37]

3. International agreements like Convention 108+, along with mutual adequacy frameworks, have opened avenues towards enhanced co-operation between regional legislations (GDPR, LGPD, CCPA). Deciding against uniform standards provides spying firms and data exporters with loopholes to exploit personal information banked in different areas of the country where protections are weak—something harmonisation would resolve.[38]

4. Revise MLATs to make them compliant with privacy policies, transparency protocols, and sparse independent judicial scrutiny for evaluating data requests. Legal frameworks are routinely ignored through back doors—bypassed directly—negating protections MLATs are meant to provide. Implement preemptive human rights impact assessments prior to authorising any cross-border surveillance actions. Users impacted should be notified and given a mechanism to contest the surveillance deemed intrusive. Standardised templates and evaluation procedures on grant/deny cross-border data access requests should be instituted.[39]

5. Enforce integration of privacy-by-design and privacy-by-default policies as fundamental requirements within 5G infrastructure and the IoT framework. Technological safeguards serve as initial lines of defence in areas where legal frameworks take time to act—or do not exist at all—and must include data minimisation and encryption alongside decentralised storage within IoT ecosystems. Promoting auditable open-source software furthers accountability while supporting PET research projects like homomorphic encryption, which increases security resiliency.[40]

6. Formulate formal partnerships between civil society organisations (CSOs) for collaborative monitoring of cross-border surveillance, extending the realms of airborne enforcement enabling capabilities while protecting jus ad bellum principles, harming the socio-political undertones, national intelligence operations, DPAs lack political independence or jurisdiction, and pose a challenge under sensitive domains.[41]

7. CSOs engage directly with litigation, advocacy, and public awareness activities. Form transnational networks of DPAs for joint investigation. Enact laws protecting whistleblowers from revealing unlawful monitoring to expose illegal surveillance. Support CSOs litigating for privacy and digital rights on international levels.[42]

8. Assist developing countries in building legal and institutional frameworks necessary to defend against foreign unwarranted surveillance.

Many developing countries do not have strong legal systems, and thus, could inadvertently permit foreign surveillance due to infrastructural agreements. Provide model legal systems coupled with workshops through international agencies like UNODC or ITU. Foster local talent in cybersecurity and privacy law. Promote regional collaboration towards resisting surveillance by advanced global powers.[43]

9. Enforce the obligation to publicly disclose the scope and limitations of intelligence sharing agreements, such as Five Eyes shorthand oversight treaties. These forms of treaties often fall under jurisdictions which lack apparent authority; therefore, accessing spy-restricted information from other nations can be used freely. Require lapsed parliamentary or judicial scrutiny for these types of agreements. Provide privacy provisions which also include means to seek remedial action and set limits on triggers which are anchored beyond reasonable expectations and responsive to specific harms rather than generalised watchful oversights.[44]

Conclusion

The establishment of 5G networks in conjunction with the rapid proliferation of IoT devices has considerably reshaped the world's digital framework by enabling unattended data transfer and exchange globally. At the same time, these changes have immensely widened the scope for both state and non-state actors to conduct extensive cross-border surveillance. National security concerns increasingly tend to justify such practices, which puts privacy as a fundamental human right under severe and continuous strain. Combating transnational surveillance requires addressing regulatory gaps at international, regional, and domestic levels. This paper seeks to demonstrate how existing legal frameworks are still far behind modern surveillance technologies. Documents of an international character, like ICCPR and UN resolutions, offer vital normative standards but lack enforcement capacity where surveillance occurs outside a nation's borders. Regarding regional safeguards under the European Convention on Human Rights or GDPR, nowadays they seem comparatively stronger by granting functions such as supervision, control mechanisms, protective boundaries alongside decisional system clarity which emerges from jurisprudence.

Nonetheless, the disparities exist in legal standards among various jurisdictions, and the unwillingness of certain states to subject their cross-border surveillance and intelligence sharing mechanisms to international scrutiny allows for the weakening of global privacy standards.

Because of its transformational nature, the digital environment prioritises the need for comprehensive revisions to legal theories covering surveillance, as well as the need to construct policies to protect privacy in a digital world. This paper seeks to contribute to the discourse on the inertia of developing international, regional, and national policies driven by surveillance capitalism, focusing instead on the reactive, siloed and unsustainable nature of these policies when compared to the challenges of global surveillance capitalism. Unlike the dominant discourse on international law, this paper positions 5G and IoT surveillance and the corresponding international legal relations within the larger international law discourse in order to assess the adequacy of doctrines of territoriality, jurisdiction, and sovereignty as they relate to the protection of privacy.

The emphasis on policy as the battleground for the contest of privacy and surveillance rights alludes to the reality that legal systems are more disparate in the extent of their enforcement, scope, and the willingness to permit oversight of their enforcement at the global level. The paper seeks to improve the dialogue by focusing on the technological dualism between developed and developing legal systems and bridging the gap between the discourse on the legal and enforceable human rights. This study also advances discourse by challenging the key legal assumptions that justify the slow regulation of surveillance within the law. By demonstrating the absence of ideal binding multilateral treaties, interoperable frameworks for cross-border data protection, and the lack of accountability, the study clarifies the need for the discourse to encompass advanced technologies. By shifting the focus from the question of cross-border privacy and associating it with determinable and abstract legal principles in transnational law, it paves the way for the study of privacy as a normative reordering of a legal system in the context of AI, IoT, and 5G technology.

References

[1] Md Nazrul Islam Khan, "Cross-Border Data Privacy And Legal Support: A Systematic Review Of International Compliance Standards And Cyber Law Practices," *American Journal of Scholarly Research and Innovation* 04, no. 01 (January 1, 2025): 138–74, https://doi.org/10.63125/a4gbeb22.

[2] Jin Su Kim, Min-Gu Kim, and Sung Bum Pan, "A Study on Implementation of Real-time Intelligent Video Surveillance System Based on Embedded Module," *EURASIP Journal on Image and Video Processing* 2021, no. 1 (November 21, 2021), https://doi.org/10.1186/s13640-021-00576-0.

[3] Andrew B. Whitford and Jeff Yates, "Surveillance and Privacy as Coevolving Disruptions: Reflections on 'Notice and Choice,'" *Policy Design and Practice* 6, no. 1 (June 15, 2022): 14–26, https://doi.org/10.1080/25741292.2022.2086667.

[4] Wang, Dan, Dong Chen, Bin Song, Nadra Guizani, Xiaoyan Yu, and Xiaojiang Du. "From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies." *IEEE Communications Magazine* 56, no. 10 (October 1, 2018): 114–20. https://doi.org/10.1109/mcom.2018.1701310.

[5] Muhammad, Khan, Tanveer Hussain, Joel J. P. C. Rodrigues, Paolo Bellavista, Antonio Roberto L. De Macedo, and Victor Hugo C. De Albuquerque. "Efficient and Privacy Preserving Video Transmission in 5G-Enabled IoT Surveillance Networks: Current Challenges and Future Directions." *IEEE Network* 35, no. 2 (December 21, 2020): 26–33. https://doi.org/10.1109/mnet.011.1900514.

[6] Taha, Miran, Lorena Parra, Laura Garcia, and Jaime Lloret. "An Intelligent Handover Process Algorithm in 5G Networks: The Use Case of Mobile Cameras for Environmental Surveillance." *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 1, 2017, 840–44. https://doi.org/10.1109/iccw.2017.7962763.

[7] United Nations (General Assembly). 1966. "International Covenant on Civil and Political Rights." *Treaty Series* 999 (December): 171

[8] United Nations. 1948. Universal Declaration of Human Rights.

[9] Zalnieriute, Monika. "Big Brother Watch V. UK: Procedural Fetishism and Mass Surveillance Under the ECHR." *Verfassungsblog: On Matters Constitutional*, June 2, 2021. https://doi.org/10.17176/20210602-123858-0.

[10] Urszula Góral, "The Right to Privacy and the Protection of Personal Data: Convention 108 as a Universal and Timeless Standard for Policymakers in Europe and Beyond," *Acta Iuris Stetinensis* 33 (January 1, 2021): 101–13, https://doi.org/10.18276/ais.2021.33-06.

[11] Council of Europe. 1981. "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." *Council of Europe Treaty Series 108*. Strasbourg: Council of Europe.

[12] United Nations General Assembly. "Resolution 68/167. The right to privacy in the digital age." (2013).

[13] United Nations General Assembly. "Resolution 73/179. The right to privacy in the digital age." (2018).

[14] Kusche, Isabel. "Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk." *Journal of Risk Research*, May 11, 2024, 1–14. https://doi.org/10.1080/13669877.2024.2350720.

[15] Rangari, Jayesh. "Balancing AI Innovation and Privacy: A Study of Facial Recognition Technologies Under the DPDPA." *Revista Review Index Journal of Multidisciplinary* 5, no. 1 (March 31, 2025): 30–38. https://doi.org/10.31305/rrijm2025.v05.n01.004.

[16] Witzleb, Normann, and Julian Wagner. "When Is Personal Data 'About' or 'Relating to' an Individual? A Comparison of Australian, Canadian and EU Data Protection and Privacy Laws." *SSRN Electronic Journal*, January 1, 2018. https://doi.org/10.2139/ssrn.3189376.

[17] Schäfer, Fabian, Heiko Gebauer, Christoph Gröger, Oliver Gassmann, and Felix Wortmann. "Data-driven Business and Data Privacy: Challenges and Measures for Product-based Companies." *Business Horizons* 66, no. 4 (October 7, 2022): 493–504. https://doi.org/10.1016/j.bushor.2022.10.002.

[18] Maximillian Schrems v. Data Protection Commissioner, Case C-362/14, Court of Justice of the European Union, Oct. 6, 2015.

[19] Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, Court of Justice of the European Union, July 16, 2020.

[20] Big Brother Watch and Others v. the United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021)

[21] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., Writ Petition (Civil) No. 494 of 2012 (India).

[22] Chettri, Lalit, and Rabindranath Bera. "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems." *IEEE Internet of Things Journal* 7, no. 1 (October 22, 2019): 16–32. https://doi.org/10.1109/jiot.2019.2948888.

[23] Saraswat, Deepti, Pronaya Bhattacharya, Arunendra Singh, Ashwin Verma, Sudeep Tanwar, and Neeraj Kumar. "Secure 5G-Assisted UAV Access Scheme in IoBT for Region Demarcation and Surveillance Operations." *IEEE Communications Standards Magazine* 6, no. 1 (March 1, 2022): 58–66. https://doi.org/10.1109/mcomstd.0001.2100057.

[24] Hui, Hongxun, Yi Ding, Qingxin Shi, Fangxing Li, Yonghua Song, and Jinyue Yan. "5G Network-based Internet of Things for Demand Response in Smart Grid: A Survey on Application Potential." *Applied Energy* 257 (October 24, 2019): 113972. https://doi.org/10.1016/j.apenergy.2019.113972.

[25] Lu, Yunlong, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT." *IEEE Transactions on Industrial Informatics* 16, no. 6 (September 18, 2019): 4177–86. https://doi.org/10.1109/tii.2019.2942190.

[26] Chanal, Poornima M., and Mahabaleshwar S. Kakkasageri. "Security and Privacy in IoT: A Survey." *Wireless Personal Communications* 115, no. 2 (July 29, 2020): 1667–93. https://doi.org/10.1007/s11277-020-07649-9.

[27] Bradford, Laura, Mateo Aboy, and Kathleen Liddell. "Standard Contractual Clauses for Cross-border Transfers of Health Data After Schrems II." *Journal of Law and the Biosciences* 8, no. 1 (January 1, 2021). https://doi.org/10.1093/jlb/lsab007.

[28] Calvo, Rafael A, Sebastian Deterding, and Richard M Ryan. "Health Surveillance During Covid-19 Pandemic." *BMJ*, April 6, 2020, m1373. https://doi.org/10.1136/bmj.m1373.

[29] Calzada, Igor. "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)." *Smart Cities* 5, no. 3 (September 8, 2022): 1129–50. https://doi.org/10.3390/smartcities5030057.

[30] Smith, Stephen W. "Clouds on the Horizon: Cross-Border Surveillance Under the US CLOUD Act." In *Hart Publishing eBooks*, 2020. https://doi.org/10.5040/9781509940691.ch-008.

[31] Ahnert, Ruth, and Sebastian E Ahnert. "Metadata, Surveillance and the Tudor State." *History Workshop Journal* 87 (November 17, 2018): 27–51. https://doi.org/10.1093/hwj/dby033.

[32] Bennett, Colin, and Oduro Marfo Smith. "Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities." *SSRN Electronic Journal*, January 1, 2019. https://doi.org/10.2139/ssrn.3517889.

[33] Singh, Tulika. "AI-Driven Surveillance Technologies and Human Rights: Balancing Security and Privacy." In *Smart Innovation, Systems and Technologies*, 703–17, 2024. https://doi.org/10.1007/978-981-97-3690-4_53.

[34] Wazid, Mohammad, Ashok Kumar Das, Sachin Shetty, Prosanta Gope, and Joel J. P. C. Rodrigues. "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap." *IEEE Access* 9 (December 28, 2020): 4466–89. https://doi.org/10.1109/access.2020.3047895.

[35] Singh, Tulika. "AI-Driven Surveillance Technologies and Human Rights: Balancing Security and Privacy." In *Smart Innovation, Systems and Technologies*, 703–17, 2024. https://doi.org/10.1007/978-981-97-3690-4_53.

[36] Georgieva, Ilina. "The Right to Privacy Under Fire – Foreign Surveillance Under the NSA and the GCHQ and Its Compatibility With Art. 17 ICCPR and Art. 8 ECHR." *Utrecht Journal of International and European Law* 31, no. 80 (February 27, 2015): 104–30. https://doi.org/10.5334/ujiel.cr.

[37] Gabriele Cosentino, "Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media" (2022) 13 Bustan the Middle East Book Review 190 <https://doi.org/10.5325/bustan.13.2.0190>.

[38] De Terwangne, Cécile. "Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data." *Computer Law & Security Review* 40 (January 14, 2021): 105497. https://doi.org/10.1016/j.clsr.2020.105497.

[39] Cortes, Sarah. "MLAT Jiu-Jitsu and Tor: Mutual Legal Assistance Treaties in Surveillance." *Richmond Journal of Law & Technology* 22, no. 1 (January 1, 2015): 2. https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1422&context=jolt.

[40] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. "IoT Privacy and Security: Challenges and Solutions." *Applied Sciences* 10, no. 12 (June 15, 2020): 4102. https://doi.org/10.3390/app10124102.

[41] Chatfield, Akemi Takeoka, Christopher G. Reddick, and Uuf Brajawidagda. "Government Surveillance Disclosures, Bilateral Trust and Indonesia–Australia Cross-border Security Cooperation: Social Network Analysis of Twitter Data." *Government Information Quarterly* 32, no. 2 (March 25, 2015): 118–28. https://doi.org/10.1016/j.giq.2015.01.002.

[42] Gineen K Abuali, "The Chilling of Religious Liberty in the Age of Digital Surveillance" (2023) 54 Seton Hall Law Review 533 <https://doi.org/10.60095/apeg7862>.

[43] Bignami F and Resta G, "Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance" [2018] SSRN Electronic Journal 357 <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3043771_code810317.pdf?abstractid=3043771&mirid=1>

[44] Shi-Cho Cha and others, "Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges" (2018) 6 IEEE Internet of Things Journal 2159 <https://doi.org/10.1109/jiot.2018.2878658>.