INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 4 | 2026 Art. 04

Artificial Intelligence, Surveillance and Transnational Regulation: Towards a Global Framework for Digital Accountability

Atul Babu
LLM Student,
Amity Law School, Amity University, Bengaluru

Johns V James
LLM Student,
Amity Law School, Amity University, Bengaluru

Recommended Citation
Atul Babu and Johns V James, *Artificial Intelligence, Surveillance and Transnational Regulation: Towards a Global Framework for Digital Accountability,* 5 IJHRLR 43-56 (2026).
Available at www.ijhrlr.in/current-issues/.

Artificial Intelligence, Surveillance and Transnational Regulation: Towards a Global Framework for Digital Accountability

ABSTRACT

Artificial intelligence has quietly become a central tool in modern surveillance. From facial recognition systems in public spaces to algorithmic monitoring of online behaviour, AI-driven surveillance now functions across borders, often without clear legal limits. While states justify such technologies in the name of security, efficiency, or governance, their use increasingly affects privacy, autonomy, and basic civil liberties at a global level. Existing legal frameworks, which are largely domestic and territorial in nature, struggle to regulate surveillance practices that are inherently transnational. This paper examines how AI-enabled surveillance exposes serious regulatory and accountability gaps when data, algorithms, and decision-making processes move across jurisdictions. It argues that fragmented national laws allow both state authorities and private technology companies to evade responsibility through jurisdictional ambiguity. Current international standards and soft-law instruments offer guidance but lack binding force and effective enforcement, leaving individuals with limited remedies against cross-border surveillance harms. Using a doctrinal and comparative legal approach, the study analyses emerging regulatory responses to AI surveillance and highlights their limitations when applied in isolation. The paper contends that meaningful accountability cannot be achieved through domestic regulation alone and calls for a coordinated global framework grounded in legal responsibility rather than technological optimism. By proposing foundational principles such as transparency, proportionality, human oversight, and cross-border cooperation, the paper seeks to reframe AI surveillance as a matter of legal accountability rather than technical governance. Ultimately, the study emphasises the need for transnational legal solutions to ensure that the expansion of AI surveillance does not come at the cost of fundamental rights.

KEYWORDS

Artificial Intelligence, Surveillance, Cross-Border Regulation, Accountability; Privacy, Human Rights, Global Legal Framework

1. INTRODUCTION

Artificial intelligence has become deeply embedded in contemporary systems of surveillance, reshaping how states and private actors collect, analyse, and act upon personal data. Unlike earlier forms of monitoring, AI-driven surveillance relies on automated decision-making, pattern recognition, and large-scale data aggregation, allowing surveillance practices to operate continuously and across borders. Facial recognition in public spaces, algorithmic risk assessment, biometric identification, and digital tracking now form part of everyday governance, often functioning invisibly and without meaningful consent. While such technologies are frequently justified on grounds of security, efficiency, or public order, their expanding use raises serious legal concerns that extend beyond domestic regulatory boundaries.

Traditional legal frameworks governing surveillance are rooted in territorial jurisdiction and state accountability. However, AI systems challenge this structure by operating within transnational digital ecosystems where data flows freely across borders, algorithms are developed in one jurisdiction and deployed in another, and decision-making authority is diffused between public institutions and private technology companies. As a result, individuals affected by AI-enabled surveillance often face uncertainty regarding which legal system applies, who is responsible for harm, and what remedies are available. This jurisdictional fragmentation creates significant accountability gaps, enabling surveillance practices to persist without adequate oversight.

The legal implications of AI surveillance are particularly acute in the context of fundamental rights. Automated surveillance technologies can interfere with privacy, freedom of expression, equality, and due process, especially when deployed at scale and without transparency. Bias embedded within algorithms, opacity in decision-making processes, and the absence of human oversight further intensify the risk of rights violations. Courts and regulators have begun to acknowledge these concerns, yet legal responses remain largely reactive and nationally confined. In a digital environment where surveillance technologies routinely transcend borders, domestic regulation alone appears insufficient to address the structural challenges posed by AI-driven monitoring[1] . At the international level, several soft-law instruments and ethical guidelines seek to promote responsible AI use. While these frameworks emphasise values such as fairness, accountability, and transparency, they lack binding force and effective enforcement mechanisms. Moreover, they often fail to address the

[1] European Court of Human Rights, *Big Brother Watch and Others v United Kingdom* (2021) 72 EHRR 17.

specific realities of surveillance technologies, particularly when deployed through public-private partnerships and transnational data infrastructures. The absence of a coherent global approach allows regulatory arbitrage, where actors exploit weaker legal regimes to deploy intrusive surveillance tools with minimal scrutiny.

This paper argues that AI-enabled surveillance must be understood as a transnational legal issue rather than a purely technological or domestic governance concern. It contends that meaningful digital accountability requires a coordinated global framework capable of addressing cross-border surveillance practices, clarifying responsibility, and ensuring protection of fundamental rights. By examining the limitations of existing regulatory approaches and exploring emerging legal responses, the study seeks to contribute to the evolving discourse on transnational AI governance and the urgent need for international legal coordination in the age of automated surveillance[2].

1.1 Research Problem

The rapid expansion of AI-enabled surveillance across borders has exposed serious gaps in existing legal frameworks, which remain largely domestic and fragmented. Surveillance technologies often operate through transnational data flows, private technology providers, and automated decision-making systems, making it difficult to identify responsibility and ensure legal accountability. Current national regulations and non-binding international guidelines fail to adequately address jurisdictional conflicts, regulatory arbitrage, and the protection of fundamental rights in cross-border surveillance practices. The central problem addressed by this research is the absence of a coherent transnational legal framework capable of regulating AI-driven surveillance while ensuring transparency, accountability, and effective remedies for rights violations.

1.2. Research Objectives

This research has several objectives:

- To examine the nature and scope of AI-enabled surveillance technologies operating across national borders.
- To analyse the legal and regulatory challenges arising from the transnational deployment of AI surveillance systems.

[2] United Nations General Assembly, *The Right to Privacy in the Digital Age* UN Doc A/RES/68/167 (2013).

- To assess the adequacy of existing domestic laws and international instruments in ensuring accountability and protection of fundamental rights.

- To study emerging regulatory approaches adopted by different jurisdictions in response to AI-driven surveillance.

- To propose core principles for a coordinated global framework aimed at ensuring transparency, accountability, and rights-based regulation of AI surveillance technologies.

1.3. Research Methodology

This research adopts a doctrinal and analytical methodology to examine the legal issues arising from AI-enabled surveillance in a transnational context. Primary sources such as international conventions, judicial decisions, regulatory instruments, and policy documents are analysed to understand existing legal approaches. Secondary sources including academic writings, journals, and expert reports are reviewed to identify accountability gaps and regulatory challenges. A comparative method is employed to study regulatory responses across different jurisdictions. The study further uses critical analysis to evaluate the adequacy of current frameworks and to develop principles for a coordinated global regulatory approach.

1.4. Scope And Limitations

The scope of this study is limited to examining AI-enabled surveillance from a transnational legal perspective, with a focus on regulatory and accountability challenges. It analyses selected international frameworks and comparative regulatory approaches rather than providing an exhaustive jurisdiction-by-jurisdiction review. The study does not engage in technical analysis of AI systems and is constrained by the evolving nature of AI regulation, which may affect the long-term applicability of its findings.

2.LITERATURE REVIEW

According to various scholarly discourse on artificial intelligence and surveillance has largely focused on the tension between technological advancement and the protection of fundamental rights. Early literature highlights how AI-driven surveillance differs from traditional monitoring due to its scale, speed, and predictive capacity, allowing authorities to collect and process personal data continuously and often invisibly[3]. Scholars argue that this shift intensifies risks to privacy and autonomy, particularly when surveillance is normalised within public

[3] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).

governance.

A significant body of literature examines the inadequacy of domestic legal frameworks in addressing AI-enabled surveillance. Authors note that national data protection and surveillance laws are rooted in territorial jurisdiction, making them ineffective against systems that rely on cross-border data flows and global technology providers [4] . This fragmentation enables regulatory arbitrage, allowing both state and private actors to deploy intrusive surveillance technologies in jurisdictions with weaker oversight mechanisms.

Several scholars emphasise the role of private corporations in transnational surveillance ecosystems. Unlike traditional state surveillance, AI systems are often developed, maintained, and operated by private entities, blurring lines of accountability[5]. This public private overlap complicates legal responsibility, as existing laws struggle to attribute liability when harm results from automated or opaque decision-making processes.

At the international level, literature on AI governance highlights the growing reliance on soft law instruments, ethical guidelines, and non-binding principles. While these frameworks promote values such as transparency and fairness, critics argue that they lack enforceability and fail to provide effective remedies for individuals affected by cross-border surveillance practices [6] .The absence of binding international standards has led scholars to call for harmonised transnational regulation grounded in human rights law. Recent studies advocate a shift towards global legal coordination, suggesting that AI surveillance should be regulated through shared principles rather than isolated domestic rules[7]. This literature forms the foundation for the present study, which builds upon existing critiques to argue for a structured global framework focused on accountability rather than technological governance alone.

3.TRANSNATIONAL ANALYSIS OF AI-ENABLED SURVEILLANCE AND ACCOUNTABILITY

Artificial intelligence–enabled surveillance presents challenges that

[4] Mireille Hildebrandt, 'Law as Computation in the Era of Artificial Legal Intelligence' (2018) 68 *University of Toronto Law Journal* 12.

[5] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001).

[6] Luciano Floridi and others, 'AI4People An Ethical Framework for a Good AI Society' (2018) 28 *Minds and Machines* 689.

[7] Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 *Regulation & Governance* 505. [8] Regulation (EU) 2016/679 (GDPR).

fundamentally transcend national borders. Unlike traditional surveillance, AI-driven monitoring systems rely on vast datasets, algorithmic decision-making, cloud infrastructures, and private technology providers operating across jurisdictions. Data may be collected in one country, processed in another, and analysed by algorithms developed elsewhere. This transnational character renders domestic legal frameworks inadequate, as accountability mechanisms remain territorially confined while surveillance practices function globally.

- ***European Union: Rights-Based Regulation with Extraterritorial Limits***

The European Union has adopted one of the most comprehensive legal frameworks addressing digital surveillance through a rights-based approach. The General Data Protection Regulation (GDPR) establishes strict principles of lawfulness, necessity, proportionality, and transparency in personal data processing, including safeguards against automated decision-making and profiling. AI-enabled surveillance technologies such as facial recognition and biometric identification fall within the GDPR's heightened protections[8].

Judicial scrutiny has reinforced these principles. In *Digital Rights Ireland Ltd v Minister for Communications*, the Court of Justice of the European Union (CJEU) invalidated the Data Retention Directive for permitting indiscriminate retention of personal data without adequate safeguards, emphasising that large-scale data collection inherently threatens fundamental rights[8]. This reasoning is particularly relevant to AI surveillance, which depends on mass data aggregation.

Similarly, in *Big Brother Watch and Others v United Kingdom*, the European Court of Human Rights (ECtHR) held that bulk interception regimes violate the right to privacy unless accompanied by strict safeguards, independent oversight, and transparency[9] . The judgment implicitly acknowledges the heightened risks posed by automated and large-scale surveillance systems.

However, despite its normative strength, the EU framework remains regionally limited. The extraterritorial application of GDPR faces enforcement challenges once data is transferred outside the EU or processed by foreign intelligence agencies. This limitation was exposed in *Schrems II*, where the CJEU invalidated the EU–US Privacy Shield due to US surveillance laws and the absence of

[8] D*igital Rights Ireland Ltd v Minister for Communications* (C-293/12) EU:C: 2014:238.

[9] *Big Brother Watch and Others v United Kingdom* (2021) 72 EHRR 17.

effective remedies for EU citizens[10]. The case illustrates how transnational surveillance undermines even robust domestic protections, reinforcing the need for coordinated global regulation.

- ***United States: Security-Oriented and Fragmented Accountability***

The United States follows a markedly different regulatory approach, prioritising national security and sector-specific regulation over comprehensive data protection. Surveillance law is shaped primarily by constitutional interpretation and national security statutes, resulting in fragmented oversight of AI-enabled monitoring.

In Carpenter v United States, the US Supreme Court recognised that prolonged access to digital location data constitutes a serious intrusion into privacy, requiring a warrant under the Fourth Amendment11.Although not directly addressing AI, the judgment acknowledges that modern surveillance technologies differ qualitatively from traditional monitoring due to their scale and predictive capacity. This reasoning is highly relevant to AI-driven surveillance systems.

Nevertheless, statutory regimes such as the Foreign Intelligence Surveillance Act (FISA) permit extensive bulk data collection, particularly involving non-US citizens who lack standing to challenge surveillance practice12s. The absence of comprehensive privacy legislation allows AI surveillance technologies developed by US companies to be exported globally with minimal accountability. From a transnational perspective, this regulatory asymmetry enables jurisdiction shopping and weakens global rights protection.

- **China: State-Centric Surveillance and Global Export**

China represents a contrasting model characterised by strong state control and widespread integration of AI surveillance into governance. Facial recognition systems, biometric databases, and predictive analytics are deployed extensively for public administration and social monitoring. While China has enacted data protection and algorithm regulation laws, these frameworks

[10] *Data Protection Commissioner v Facebook Ireland Ltd* (C-311/18) EU:C: 2020:559 (*Schrems II*).

[11] C*arpenter v United States* 585 US (2018)

[12] Personal Information Protection Law 2021 (China).

prioritise state objectives over individual rights.[13]

The transnational implications of China's model are particularly significant due to the export of AI surveillance technologies to other states. Surveillance infrastructure supplied through international partnerships often lacks transparency and rights safeguards, enabling recipient countries to adopt intrusive monitoring practices without robust legal oversight [14] . This illustrates how divergent regulatory philosophies can weaken global accountability when surveillance technologies circulate transnationally.

- ***International Human Rights Law and Soft-Law Governance***

At the international level, responses to AI surveillance rely predominantly on human rights instruments and soft-law frameworks. United Nations resolutions affirm that privacy and other fundamental rights apply equally in the digital sphere and caution against unlawful or arbitrary surveillance[15]. However, such instruments are non-binding and lack enforcement mechanisms. Judicial engagement at the international level remains limited. In *Roman Zakharov v Russia*, the ECHR condemned secret surveillance regimes lacking adequate safeguards, stressing that unchecked monitoring powers pose systemic risks to democracy[15]. While the case strengthens rights-based reasoning, its impact remains confined to member states and does not address transnational surveillance directly. Similarly, OECD AI Principles and UNESCO's AI ethics recommendations promote transparency, accountability, and human-centred governance[16]. Yet their voluntary nature allows states and corporations to selectively adopt principles without meaningful compliance, perpetuating regulatory fragmentation.

- ***The Transnational Accountability Gap***

Across jurisdictions, a consistent accountability gap emerges. Surveillance systems operate through complex networks involving governments, private technology firms, cloud service providers, and data brokers located in multiple jurisdictions. Existing legal frameworks focus primarily on state responsibility and fail to adequately regulate private actors who design, deploy, and maintain

[13] UN Human Rights Council, *Report on the Right to Privacy in the Digital Age* UN Doc A/HRC/48/31 (2021).

[14] UN General Assembly, *The Right to Privacy in the Digital Age* UN Doc A/RES/73/179 (2018). [15] *Roman Zakharov v Russia* (2015) 63 EHRR 17.

[15] OECD, *Principles on Artificial Intelligence* (2019).

[16] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015). [19] Personal Information Protection Law 2021 (China).

AI surveillance technologies.

Courts struggle to assign liability when harm results from algorithmic decision-making distributed across borders. States invoke national security exceptions, while private actors claim technological neutrality. Individuals affected by transnational surveillance are left without effective remedies, as jurisdictional barriers prevent meaningful legal redress. This structural gap demonstrates the insufficiency of territorially bounded regulation.

- ***Towards a Global Framework for Digital Accountability***

The comparative and judicial analysis demonstrates that no jurisdiction has successfully addressed AI-enabled surveillance at the transnational level. While the EU emphasises rights, the US prioritises security, and China advances state control, none provide a comprehensive solution to cross-border accountability. This fragmentation underscores the need for a coordinated global framework grounded in legal responsibility rather than technological governance. Such a framework must establish shared principles of transparency, proportionality, human oversight, and clear attribution of responsibility across jurisdictions. Binding international standards, cross-border regulatory cooperation, and enforceable remedies are essential to ensure that AI-enabled surveillance does not erode fundamental rights in an interconnected digital environment[19].

4. CRITICAL DISCUSSIONS AND ANALYSIS

The transnational expansion of AI-enabled surveillance exposes a fundamental mismatch between the global operation of digital technologies and the territorially bound nature of law. Existing regulatory responses remain fragmented, with states adopting divergent approaches shaped by domestic priorities such as security, economic competitiveness, or social control. While jurisdictions like the European Union attempt to embed rights-based safeguards within AI governance, others prioritise national security or state authority, resulting in regulatory asymmetry. This fragmentation weakens accountability by allowing surveillance actors to exploit jurisdictional gaps and relocate data processing or deployment to less restrictive legal environments.

A critical concern lies in the reliance on soft-law mechanisms and ethical frameworks at the international level. Although these instruments promote transparency, fairness, and accountability, their non-binding nature limits their capacity to restrain intrusive surveillance practices.

Ethical guidelines often assume voluntary compliance and technological neutrality, failing to address power imbalances between states, corporations, and individuals. In the context of AI surveillance, where decision-making is automated and opaque, such reliance risks legitimising harmful practices without providing enforceable remedies.

Judicial interventions have contributed valuable normative principles, particularly in affirming privacy and proportionality in surveillance regimes. However, courts remain constrained by jurisdictional boundaries and evidentiary limitations. Decisions addressing mass surveillance, such as those delivered by European courts, emphasise safeguards and oversight but struggle to regulate cross-border surveillance operations involving foreign intelligence agencies or multinational corporations. As a result, judicial protection remains reactive rather than preventive, addressing violations only after harm has occurred.

Another critical issue is the blurred line between public and private actors in AI surveillance ecosystems. Private technology companies increasingly design, operate, and export surveillance systems, yet legal frameworks continue to focus primarily on state responsibility. This disconnect enables private actors to evade accountability by positioning themselves as neutral service providers, despite exercising significant influence over surveillance capabilities and outcomes. Without clear transnational obligations imposed on private entities, accountability remains incomplete.

Ultimately, the persistence of these challenges demonstrates that domestic regulation and soft law governance are insufficient to address the structural risks posed by AI-enabled surveillance. [17]A shift towards binding transnational legal coordination is necessary, one that recognises surveillance as a shared global concern rather than a sovereign prerogative. Such an approach must prioritise enforceable accountability, clarify responsibility across borders, and ensure that technological advancement does not undermine fundamental rights in the digital age[18].

5. FINDINGS AND DISCUSSIONS

First, fragmentation is still the rule rather than the exception. Each jurisdiction follows its own path shaped by its political and legal culture: the EU sets detailed rules, the US relies on flexibility, China favours centralised control, and India walks a cautious middle line. No single global model has emerged. Second, global standards exist in theory but

[17] *Big Brother Watch and Others v United Kingdom* (2021) 72 EHRR 17

[18] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015).

not in practice. Softlaw instruments like OECD principles and FATF guidance help shape conversations, but they are not binding on states. Their value depends on whether countries choose to adopt them, and at present uptake is inconsistent. Third, different regulatory philosophies create tensions. Europe seeks to prevent risk upfront, while the US acts only after harms occur. Similar differences exist in crypto policy. These approaches aren't easy to reconcile, but they do highlight potential shared ground such as stronger disclosure rules and coordinated anti–money laundering measures. Fourth, regulation must evolve with technology. Courts and human rights bodies have stepped in when outdated frameworks fall short, showing why flexible mechanisms like regulatory sandboxes and periodic reviews can make policies more resilient. Finally, global cooperation is necessary but still emerging. Discussions through forums like the G20 and OECD show growing recognition that unilateral action isn't enough. The fact that major states from China to India are now openly exploring coordination suggests gradual harmonisation is possible, though still a work in progress.

6. CONCLUSION AND RECOMMENDATIONS

AI-enabled surveillance has reshaped governance by enabling large-scale, automated monitoring that operates across national borders. This study has shown that existing legal frameworks remain fragmented and territorially confined, making them inadequate to regulate transnational surveillance practices. While some jurisdictions have adopted rights-oriented approaches, others prioritise security or state control, resulting in regulatory asymmetry and accountability gaps. Judicial interventions and international soft-law instruments offer important normative guidance but lack comprehensive reach and enforceability. The absence of coordinated global regulation allows surveillance technologies to expand with limited oversight, posing serious risks to privacy, autonomy, and fundamental rights in the digital age.

- To address the regulatory deficiencies identified in this study, a shift towards coordinated transnational governance of AI-enabled surveillance is essential. First, there is a need for the development of a binding international legal framework specifically addressing AI-driven surveillance. Such a framework should move beyond voluntary ethical guidelines and establish enforceable obligations for states, intelligence agencies, and private technology providers involved in surveillance operations. Binding standards would reduce regulatory arbitrage and ensure minimum protections across jurisdictions.

- Common substantive principles must form the foundation of transnational regulation. These should include legality, necessity, and proportionality in the deployment of surveillance technologies, alongside mandatory transparency regarding the use of AI systems. States should be required to disclose the scope, purpose, and safeguards governing AI surveillance, subject to narrowly defined national security exceptions.

Transparency is crucial to preventing misuse and enabling public and judicial scrutiny.

- Human oversight must be legally mandated in all AI-enabled surveillance systems. Automated decision-making should not operate independently in contexts that affect fundamental rights. Clear rules should require meaningful human review of surveillance decisions, particularly where outcomes may lead to law enforcement action, profiling, or restriction of individual freedoms. This would reduce the risks posed by algorithmic bias, error, and opacity.

- Private technology companies must be directly regulated under transnational law. Surveillance technologies are increasingly designed, operated, and exported by private actors, yet accountability mechanisms remain state-focused. International standards should impose due diligence obligations on companies, including impact assessments, audit requirements, and liability for rights violations arising from the deployment of AI surveillance tools.

- Cross-border cooperation among regulatory and supervisory authorities should be strengthened. States should establish mechanisms for information sharing, joint investigations, and mutual recognition of enforcement actions. Such cooperation would enhance the effectiveness of oversight and prevent jurisdictional loopholes from undermining accountability.

- Accessible remedies for affected individuals must be prioritised. Transnational regulatory frameworks should ensure that individuals subjected to unlawful or disproportionate AI surveillance have access to effective legal remedies, regardless of nationality or location. Without enforceable rights and remedies, digital accountability remains theoretical rather than practical.

Together, these recommendations aim to ensure that AI-enabled surveillance is governed by law, accountability, and respect for fundamental rights rather than unchecked technological expansion.

6.BIBLIOGRAPHY

1. Primary Sources

- Foreign Intelligence Surveillance Act 1978 (United States)
- Personal Information Protection Law 2021 (China)
- Regulation (EU) 2016/679 of the European Parliament and of the Council
- (General Data Protection Regulation)
- OECD, *Principles on Artificial Intelligence* (2019)
- UN General Assembly, *The Right to Privacy in the Digital Age* UN Doc A/RES/73/179 (2018)
- UN Human Rights Council, *Report on the Right to Privacy in the Digital Age* UN DocA/HRC/48/31 (2021)

2. Secondary Sources

- Floridi L and others, 'AI4People An Ethical Framework for a Good AI Society' (2018) 28 *Minds and Machines* 689
- Hildebrandt M, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015)
- Lyon D, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001)
- Yeung K, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 *Regulation & Governance* 505
- Zuboff S, *The Age of Surveillance Capitalism* (Profile Books 2019)
- Brownsword R, *Law, Technology and Society: Re-Imagining the Regulatory Environment* (Routledge 2019)
- De Hert P and Papakonstantinou V, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 *Computer Law & Security Review* 179
- Kuner C, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013)
- Mittelstadt B, Allo P, Taddeo M, Wachter S and Floridi L, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 *Big Data & Society* 1
- Ohm P, 'The Rise and Fall of Invasive ICT Surveillance' (2015) 96 *Boston University Law Review* 1417.