

DIGITAL SURVEILLANCE, PRIVACY RIGHTS, AND INTERNATIONAL HUMAN RIGHTS LAW IN THE 21ST CENTURY*

Abstract

The proliferation of digital surveillance technologies in the twenty-first century has generated profound tensions with the international human right to privacy. This article employs doctrinal legal methodology to examine the normative framework governing digital surveillance under international human rights law, with particular attention to Article 17 of the International Covenant on Civil and Political Rights, Article 8 of the European Convention on Human Rights, and the jurisprudence of the Human Rights Committee, the European Court of Human Rights, and the Court of Justice of the European Union. The article analyses the definitional scope of the right to privacy in digital environments; maps State obligations regarding legality, necessity, and proportionality of surveillance measures; interrogates the extraterritorial dimensions of digital surveillance; evaluates the intersection of surveillance with other fundamental rights including freedom of expression and non-discrimination; and critically assesses the challenges posed by mass surveillance programmes, commercial data exploitation, and artificial intelligence-enabled surveillance. The article concludes that the existing framework of international human rights law, while providing a sufficient normative foundation, requires significant institutional reinforcement, modernization of treaty interpretation, and genuine political commitment from States to curb the excesses of the surveillance state and its commercial analogues.

Keywords: Digital Surveillance, Right to Privacy, International Human Rights Law, Data Protection; Extraterritorial Jurisdiction, 21st Century

1. Introduction

Edward Snowden leaked in June 2013 to the rest of the world the existence of PRISM, XKeyscore, and a slew of other government spying programmes run by the United States National Security Agency (NSA) and other Five Eyes nations, a system of mass digital surveillance of unprecedented scale.¹ The disclosures set off an international legal and political controversy that led to the adoption of Resolution 68/167 by the United Nations General Assembly in six months, which states that the rights enjoyed offline should also be protected online, including the right to privacy.² The right to privacy in the digital age is in a complex position between the capacity of technology, the needs of national security, the interests of commerce, and fundamental rights. Digital communications technologies generate enormous amounts of information about people: who they hang out with, where they go, what they believe, how they behave in their personal lives, etc. which can be collected, stored, analyzed and shared, on a global scale, at (almost) no cost. This ability has led to what the UN's High Commissioner for Human Rights has termed as the 'unprecedented surveillance potential'.³ In spite of these developments, the major international laws pertaining to privacy were written long before the internet age. The International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR) were not intended to regulate mass surveillance of communications. A central question in international human rights law is whether the law as it stands and along with the general comments of the treaty bodies, reports of the special rapporteurs, and a growing jurisprudence, is sufficient to govern the monitoring processes of 21st century states and corporations. The article continues with a doctrinal examination of foundational documents, judicial rulings, treaty body rulings and academic commentary.

2. The Normative Scope of the Right to Privacy in Digital Environments**Foundational Instruments**

The right to privacy is guaranteed in a variety of international documents. Article 12 of the Universal Declaration of Human Rights (UDHR) says nothing about arbitrary interference with a person's privacy, family, home, or correspondence, or attacks upon honour and reputation.⁴ The treaty, which is binding on 173 States party, confers this protection treaty force on Article 17 of the ICCPR, provided no person shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour or reputation, and everyone has the right to the protection of the law against such interference or attacks.⁵ In the regional level, Article 8 of the ECHR establishes a right to respect private and family life, home and correspondence, the interference with which is allowed only for specific legitimate aims and when it is 'necessary in a democratic society'.⁶ The EU Charter of Fundamental Rights makes a distinction between the right to private and family life (Article 7)⁷ and the right to protection of personal data (Article 8),

*By **Helen Ekwutosi PARKINSON, PhD, PhD**, Faculty of Law, Nigerian British University, Email: parkinsonchambers09@gmail.com | parkinson.helen@nbu.edu.ng

¹ Edward Snowden, *Permanent Record* (Macmillan, 2019) 1–3. See also Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Metropolitan Books, 2014) 95–100.

² United Nations General Assembly, *The right to privacy in the digital age*, UN Doc A/RES/68/167 (18 December 2013).

³ Office of the United Nations High Commissioner for Human Rights (OHCHR), *The Right to Privacy in the Digital Age*, UN Doc A/HRC/27/37 (30 June 2014) (OHCHR 2014 Report) para 19.

⁴ Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217A (III) (UDHR), art 12.

⁵ International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 17.

⁶ European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953) ETS No 005 (ECHR), art 8.

⁷ Charter of Fundamental Rights of the European Union [2000] OJ C364/1, arts 7

which is a sui generis fundamental right.⁸ Other conventions that guarantee privacy are the American Convention on Human Rights and the African Charter system, but these have not seen the same jurisprudential elaboration in the digital sphere.⁹

Digital Extension of Privacy

In General Comment No 16, the Human Rights Committee ruled that the interference with privacy covered under Article 17 is not limited to physical or traditional methods of interception, but extends to ‘all forms’.¹⁰ Electronic communications are part of the correspondence. Collection, retention and processing of personal information by the State or private actors may be considered interference with the right to privacy.¹¹ In 2014, the OHCHR's report on privacy in the digital age, gave authoritative guidance that communications metadata – the data surrounding communication, such as the person to person, time, length and place – can be as informative as the content, if not more so. By compiling metadata, it is possible to create comprehensive profiles of people, track their social connections, political ideologies, health issues, and romantic connections. Not only does the report confirm the collection and retention of metadata is an interference with Article 17 of the ICCPR, it also expresses the same view about access to the content of communications.¹² It is similar to the reasoning of the European Court of Human Rights in a number of decisions, including *Malone v United Kingdom*,¹³ which concluded that the metering of telephone calls, the logging of the numbers dialled, was protected by Article 8 of the ECHR. More recently, the ECtHR in *Big Brother Watch and Others v United Kingdom*¹⁴ held that bulk interception regimes, mass interception of Internet communications, would always be an interference on Article 8 rights, even if the material gathered is later reviewed by a human being.¹⁵

Privacy and Human Dignity

Common to most of the scholarly literature and the output of the treaty bodies is the linking of the right to privacy to the concept of human dignity and personal autonomy. Kirsty Hughes has maintained that privacy allows people to manage the information context in which they live, and thus helps preserve the conditions for their independent self-development.¹⁶ In her work on surveillance capitalism, Shoshana Zuboff illuminates the extent to which data is harvested by private companies and turned into a raw material for products that can predict human behaviour, which ultimately undermines the autonomy and dignity of humans without their true consent.¹⁷ The intimate connection between privacy and the conditions of a free and dignified life is recognised in international law. The Human Rights Committee has repeatedly stated that privacy is not only a personal right but a social good, which allows for the emergence of the authentic personality, political participation and exercise of other fundamental rights. The right to privacy is thus a prerequisite to and underpinning of the overall structure of international human rights protection.¹⁸

3. State Obligations: Legality, Necessity, and Proportionality

The Tripartite Test

International human rights law permits interference with the right to privacy only where three cumulative conditions are satisfied: (i) the interference must have a basis in domestic law of sufficient accessibility and foreseeability (the legality requirement); (ii) the interference must pursue a legitimate aim; and (iii) the interference must be necessary and proportionate to that aim.¹⁹ These conditions apply with equal force to digital surveillance measures.²⁰

Legality

The legality requirement is not only that the surveillance be subject to the authorization of some internal legal mechanism, but that such law be accessible to citizens, predictable in its application and provide adequate procedural protection against

⁸ American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123, art 11.

⁹ Charter of Fundamental Rights of the European Union [2000] OJ C364/1, arts 8. See also; African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) 1520 UNTS 217, art 5 (human dignity); Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019), Principle 40.

¹⁰ Human Rights Committee, *General Comment No 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17)*, UN Doc HRI/GEN/1/Rev.9/Vol.I (1988) para 1.

¹¹ Human Rights Committee, *General Comment No 16* (n 5) para 8.

¹² *Ibid* para 20. See also Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/HRC/23/40 (17 April 2013) para 33.

¹³ *Malone v United Kingdom*, App No 8691/79 (ECtHR, 2 August 1984) para 64.

¹⁴ *Big Brother Watch and Others v United Kingdom*, App Nos 58170/13, 62322/14, 24960/15 (ECtHR Grand Chamber, 25 May 2021) para 347.

¹⁵ *Supra*

¹⁶ Kirsty Hughes, ‘A Behavioural Understanding of Privacy and Its Implications for Privacy Law’ (2012) 75 *Modern Law Review* 806, 808.

¹⁷ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019) 8–11.

¹⁸ *Ibid*.

¹⁹ OHCHR 2014 Report (n 7) para 25.

²⁰ Human Rights Committee, *General Comment No 16* (n 5) para 7; UN Special Rapporteur on the Right to Privacy, *Report on Privacy and Personality*, UN Doc A/HRC/40/63 (27 February 2019) para 14.

abuse.²¹ In the seminal case of *Klass and Others v Germany*,²² the European Court of Human Rights (ECHR) has accepted that secret surveillance can be compatible with the ECHR, provided robust domestic law and procedures restrain its use, ensure independent oversight over it and include notification procedures where feasible without undermining the aim of the surveillance. The Court's following decisions have developed minimum standards for legal measures allowing for surveillance: the type of offences that can justify a surveillance measure; the scope of the persons open to the surveillance; the time limit on the surveillance; the means of data storage, access, use and destruction; and the need for independent supervision of the surveillance.²³ In *Big Brother Watch*, the Grand Chamber held that the United Kingdom's bulk interception regime (as in place under the Regulation of Investigatory Powers Act 2000) failed to respect the boundaries of Article 8 because it failed to provide 'end-to-end safeguards' covering the selection of communications for interception.²⁴

Necessity and Proportionality

The necessity requirement means that surveillance must be the least intrusive way to achieve the legitimate aim sought. The proportionality requirement means that a balance should exist between individuals' rights and the interests of society as a whole. Both of these requirements become more difficult to meet where mass surveillance programs involve the collection of communications from millions of individuals without specific individual suspicion.²⁵ This challenge was addressed directly by the Court of Justice for the European Union (CJEU) in *Digital Rights Ireland*, which annulled the EU's Data Retention Directive on the basis that it did not meet proportionality requirements established by Articles 7 and 8 of the EU Charter. In particular, the CJEU noted that the Data Retention Directive provided for the collection of all traffic data from all subscribers without distinction or exception and did not contain objective criteria for limiting access by competent national authorities to these data.²⁶ The reasoning of the CJEU in *Digital Rights Ireland* has been further confirmed in *Tele2 Sverige*²⁷ and *La Quadrature du Net*,²⁸ which have established that the general and indiscriminate retention of communications data is fundamentally incompatible with EU fundamental rights law.²⁹ The OHCHR has concluded, based on its interpretation of the ICCPR framework, that bulk surveillance programs will almost inevitably never meet the necessity and proportionality requirements because they do not target identifiable individuals.³⁰

Oversight and Accountability

To comply with the obligation of ensuring independent and effective oversight of surveillance activities, States are required to establish supervision mechanisms which are independent of the authorities involved in carrying out such surveillance. The Human Rights Committee in its General Comment No 16 states that the limiting interference with an individual's right to privacy must be subject to 'effective control' and thereby interferences must be subject to some form of independent judicial oversight.³¹ The Special Rapporteur on the Right to Privacy has outlined specific principles to ensure adequate oversight over national security intelligence activities that require some form of independent assessment by the judiciary and other entities.³² In particular, effective judicial oversight has become a focal point of discussion at the European Court of Human Rights in *Szabó and Vissy v Hungary*,³³ where the ECHR determined that the system of secret surveillance laws in Hungary constitutes a violation of Article 8, in part, because the independent oversight body did not have power or authority to provide advance permission or to prevent any surveillance operations. Furthermore, the ECHR has repeatedly confirmed that states must have prior judicial approval (not simply approval by the Executive) as a minimum standard for preventing abuse of a state's powers over an individual's privacy.³⁴

4. Extraterritorial Dimensions of Digital Surveillance

The Jurisdictional Challenge

Digital surveillance is inherently transnational: data transits multiple jurisdictions, intelligence agencies intercept communications of foreign nationals abroad, and data stored in one country may be accessed by authorities in another. The

²¹ Human Rights Committee, *General Comment No 16* (n 5) para 4; see also *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* [2019] UKIPTrib IPT_14_85-CH (UK Investigatory Powers Tribunal).

²² *Klass and Others v Germany*, App No 5029/71 (ECtHR, 6 September 1978) para 50.

²³ *Szabó and Vissy v Hungary*, App No 37138/14 (ECtHR, 12 January 2016) paras 68–73.

²⁴ *ibid* paras 350–360.

²⁵ UN General Assembly, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, UN Doc A/HRC/39/29 (3 August 2018) para 10.

²⁶ *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (Joined Cases C-293/12 and C-594/12) EU: C: 2014:238 [2014] (CJEU, 8 April 2014) para 37.

²⁷ *Tele2 Sverige AB v Post-och telestyrelsen* (Joined Cases C-203/15 and C-698/15) EU: C: 2016:970 [2016] (CJEU Grand Chamber, 21 December 2016) para 100.

²⁸ *La Quadrature du Net and Others v Premier ministre and Others* (Joined Cases C-511/18, C-512/18, C-520/18) EU: C: 2020:791 [2020] (CJEU Grand Chamber, 6 October 2020) para 168.

²⁹ *Supra*

³⁰ OHCHR 2014 Report (n 7) para 26; see also Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (2nd edn, NP Engel, 2005) 381.

³¹ Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, *Principles for Oversight of National Security Intelligence*, UN Doc A/71/368 (8 September 2016) para 18.

³² Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, *Principles for Oversight of National Security Intelligence*, UN Doc A/71/368 (8 September 2016) para 18.

³³ *Szabó and Vissy v Hungary*, No. 37138/14, ECtHR

³⁴ *Supra*

application of international human rights law to extraterritorial digital surveillance raises fundamental questions about the jurisdictional reach of human rights treaty obligations.³⁵ The orthodox position, reflected in the text of the ICCPR and the jurisprudence of the Human Rights Committee, is that States' obligations extend to individuals 'within [their] territory and subject to [their] jurisdiction' (Article 2(1) ICCPR). However, the Committee in General Comment No 31 confirmed that jurisdiction may in certain circumstances extend to persons abroad who are subject to the effective control of State agents.³⁶

The NSA Disclosures and the Jurisdictional Debate

The Snowden disclosures pushed this topic from theory to real life. The NSA was using the PRISM program to gather data on non-US citizens who were stored on servers in the US (since they had a US server). The NSA was also using XKeyscore to intercept Internet communications around the world at fibre optic cables. Therefore, it was a question as to whether or not the non-US citizens being surveilled were entitled to any form of protection from the ICCPR (International Covenant on Civil and Political Rights).³⁷ Marko Milanovic has convincingly argued that a functional (rather than spatial - where you are physically located) based approach to jurisdiction (based on whether or not you were able to exercise control over a person and their rights) best serves the purpose of international human rights law and is consistent with increasing practice/interpretation by international treaty bodies.³⁸ In the Human Rights Committee (HR Committee) 2014 concluding observations regarding the United States that the HR committee expressed concern about how the NSA surveillance program(s) compromised the privacy rights of non-US citizens, and called on the US to ensure that the surveillance activities they are conducting both inside and outside the US comply with their ICCPR obligations.³⁹ The European Court of Human Rights ('ECtHR') has taken up the issue of the extent to which a state has jurisdiction over its nationals in the case of *Centrum för rättvisa v Sweden*.⁴⁰ In this case the ECtHR found that bulk interception of cable communications by Swedish intelligence agencies had the effect of intercepting the communication of both persons within and outside of Sweden, and so involved the jurisdiction of Sweden under the European Convention on Human Rights ('ECHR'). The ECtHR recognized the difficulty in determining the point at which a state loses its jurisdiction.⁴¹

International Data Transfers and Human Rights

A related dimension concerns the transfer of personal data between States and to third countries. The CJEU in *Schrems I* invalidated the EU-US Safe Harbour arrangement on the ground that it failed to ensure a level of protection equivalent to that guaranteed by the EU Charter, finding in particular that US national security law permitted authorities to access personal data transferred from the EU on a generalised basis incompatible with EU fundamental rights.⁴² In *Schrems II*, the Court invalidated the successor Privacy Shield framework on the same basis, confirming that national security access that goes beyond what is strictly necessary and proportionate is incompatible with fundamental rights.⁴³ These judgments carry significant implications for international human rights law more broadly. They affirm that the transfer of data to a third country cannot be used to circumvent fundamental rights guarantees, a principle with clear purchase in the ICCPR framework under the general obligation of States not to expose individuals to violations of their Covenant rights through international transfers of information.⁴⁴

5. Digital Surveillance and Its Intersection with Other Fundamental Rights

Freedom of Expression and the Chilling Effect

Digital surveillance and freedom of expression is one of the great human rights issues of the digital age. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) guarantees freedom of expression, not just the right to communicate information and ideas, but also the right to access information and ideas without interference.⁴⁵ Digital surveillance practices, such as mass interception of communications, monitoring of online activity, data retention programmes, and tracking of internet usage can have a negative impact on this freedom by fostering what has been called the 'chilling effect'.⁴⁶ In a highly cited report submitted to the United Nations Human Rights Council in 2013, the then UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, found that people who feel their communications are under surveillance are more likely to change their behaviour, to avoid

³⁵ Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 *Harvard International Law Journal* 81, 84.

³⁶ Human Rights Committee, *General Comment No 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, UN Doc CCPR/C/21/Rev.1/Add.13 (2004) para 10.

³⁷ Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford University Press, 2011) 207–211.

³⁸ *Ibid.*

³⁹ Human Rights Committee, *Concluding Observations on the United States of America*, UN Doc CCPR/C/USA/CO/4 (23 April 2014) para 22.

⁴⁰ *Centrum för rättvisa v. Sweden* [GC], App No 35252/08, ECHR 2021

⁴¹ *Supra*

⁴² *Schrems v Data Protection Commissioner* (Case C-362/14) EU: C: 2015:650 [2015] (CJEU, 6 October 2015) para 73.

⁴³ *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Case C-311/18) EU: C: 2020:559 [2020] (CJEU Grand Chamber, 16 July 2020) (*Schrems II*) para 197.

⁴⁴ OHCHR, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, UN Doc A/HRC/27/37 (30 June 2014) para 34.

⁴⁵ Article 19 of the International Covenant on Civil and Political Rights (ICCPR)

⁴⁶ United Nations Human Rights Committee, *International Covenant on Civil and Political Rights* (1966), Articles 17 and 19.

discussing sensitive issues and not to participate in legitimate political debates.⁴⁷ This type of self-censorship undermines democratic participation, stifles the free flow of ideas, and ultimately fosters a shortage of a marketplace for ideas which is integral to a democratic society. These technologies of surveillance can allow governments and private parties to easily gather a tremendous amount of personal data with little effort in the digital realm, making the chilling effect so strong that people often fear their information might be captured or leaked.⁴⁸

Journalists, human rights activists, political activists, whistleblowers and opposition members who use confidential communications to ensure their freedom of expression are particularly affected by the impact of surveillance on freedom of expression. Inability to trust that emails, phone calls, social media (or encrypted communication) may not be viewed prevents people from reporting misconduct, revealing corruption or criticizing government policy.⁴⁹ Sources may be reluctant to supply information to reporters, thereby reducing the ability of reporters to conduct investigations and hold the government accountable. International human rights institutions have repeatedly stated that any measures of surveillance should be lawful, necessary and proportionate, in accordance with Article 19(3) of the ICCPR.⁵⁰ The Human Rights Committee has established that any limitation on freedom of expression must be laid down by law, have a legitimate aim (e.g. national security or public order) and be the least intrusive method of achieving an aim. It is, therefore, difficult to reconcile with international human rights standards broad or indiscriminate surveillance programmes without proper legal protections. Not just in theory, but many of the disclosures about state surveillance programs have shown how far states can go with monitoring and its ability to silence opposition, intimidate critics, and deter civic participation.⁵¹

Furthermore, surveillance and freedom of expression are not distinct concepts but rather interconnected, underscoring the interdependence of human rights in the digital age. The right to privacy (under ICCPR, Article 17) is a key bearer of the enjoyment of freedom of expression, freedom of association and political participation. People might be reluctant to join advocacy groups, to take part in political action, attend public protests, or publish online opinions about controversial topics when they feel their privacy is being violated by excessive surveillance.⁵² The risks have been highlighted by United Nations Special Rapporteurs on Freedom of Expression and on Privacy, who have repeatedly urged for effective remedies against unlawful surveillance, transparency requirements, judicial authorization procedures and strong oversight mechanisms. This is important to prevent abuses of surveillance powers and to avoid using legitimate security concerns as a cover for infringing on fundamental freedoms. In democratic societies, the protection of freedom of expression is not just meant to mean no censorship but also that there is an environment where those who wish to communicate, discuss and exchange ideas can do so without having to worry about being constantly monitored or treated with hostility.⁵³

Freedom of Association and Political Participation

Digital surveillance poses significant challenges to the rights to freedom of association, peaceful assembly, and political participation, all of which are fundamental pillars of democratic governance. These rights are protected under Articles 21 and 22 of the International Covenant on Civil and Political Rights (ICCPR) and Article 11 of the European Convention on Human Rights (ECHR). Freedom of association enables individuals to join political parties, trade unions, civil society organizations, and advocacy groups to pursue common interests and participate in public affairs.⁵⁴ However, when governments employ surveillance technologies to monitor meetings, communications, membership records, or online activities of such groups, individuals may become reluctant to engage in collective action. The fear of being identified, monitored, profiled, or subjected to reprisals can discourage participation in legitimate political activities and weaken democratic engagement. As a result, surveillance not only affects individual privacy but also undermines the collective exercise of civil and political rights that are essential for accountability, pluralism, and public participation in governance.⁵⁵ Historical experience and contemporary evidence demonstrate that surveillance measures are frequently directed toward groups perceived as politically sensitive or critical of governmental policies. Political opposition movements, trade unions, minority communities, human rights defenders, journalists, and civil society organizations have often been subjected to disproportionate monitoring under the justification of maintaining national security or public order.⁵⁶ Such practices can have a profound chilling effect on civic participation by creating an atmosphere of fear and distrust. Individuals may avoid attending meetings, participating in protests, joining advocacy organizations, or expressing support for political causes if they believe their activities are being monitored by state authorities.⁵⁷ The United Nations Human Rights Committee has emphasized that restrictions on freedom of association and assembly must satisfy the principles of legality, necessity, and proportionality, meaning that any surveillance measures affecting these rights must be clearly authorized by law, pursue a

⁴⁷ Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/23/40 (2013).

⁴⁸ United Nations Human Rights Council, Resolution 34/7 on the Right to Privacy in the Digital Age (2017).

⁴⁹ Human Rights Committee, General Comment No. 34, *Article 19: Freedoms of Opinion and Expression*, CCPR/C/GC/34 (2011).

⁵⁰ Article 19(3) of the ICCPR, 1966.

⁵¹ Human Rights Committee, General Comment No. 34, *Article 19: Freedoms of Opinion and Expression*, CCPR/C/GC/34 (2011).

⁵² *Ibid.*

⁵³ Office of the United Nations High Commissioner for Human Rights (OHCHR), *The Right to Privacy in the Digital Age* (2014).

⁵⁴ Articles 21 and 22 of the International Covenant on Civil and Political Rights (ICCPR) and Article 11 of the European Convention on Human Rights (ECHR)

⁵⁵ Council of Europe, *European Convention on Human Rights* (1950), Article 11.

⁵⁶ Human Rights Committee, General Comment No. 37, *Right of Peaceful Assembly* (CCPR/C/GC/37, 2020).

⁵⁷ Human Rights Committee, General Comment No. 25, *Participation in Public Affairs and the Right to Vote* (CCPR/C/21/Rev.1/Add.7, 1996).

legitimate objective, and represent the least intrusive means available.⁵⁸ Indiscriminate or mass surveillance programs are therefore difficult to justify under international human rights standards because of their potential to suppress lawful political engagement and civic activism.⁵⁹

The dangers associated with unchecked surveillance became particularly evident through the Pegasus spyware scandal, which revealed the extensive capabilities of advanced commercial surveillance technologies. Developed by the Israeli cyber-intelligence company NSO Group, Pegasus spyware was reportedly used by various state actors to infiltrate the mobile devices of journalists, human rights lawyers, political opponents, activists, and even heads of state. The revelations highlighted how sophisticated surveillance tools can be exploited to undermine democratic processes, intimidate critics, and interfere with the work of individuals who play vital roles in promoting transparency and accountability.⁶⁰ In response to growing concerns, Joseph Cannataci and other international human rights experts called for a moratorium on the sale, transfer, and use of surveillance technologies until effective legal safeguards, independent oversight mechanisms, and human rights protections are established. Such measures are necessary to prevent abuse, ensure accountability, and preserve the freedoms of association and political participation that are indispensable to democratic societies.⁶¹ The growing commercialization of surveillance technologies underscores the urgent need for international regulation that balances legitimate security interests with the protection of fundamental human rights in the digital age.⁶²

Non-discrimination and Equality

Mass surveillance systems have been shown to operate in systematically discriminatory ways, with racial, ethnic, and religious minorities subject to disproportionate targeting. The profiling algorithms employed in predictive policing and counterterrorism surveillance reproduce and amplify existing social biases embedded in training data.⁶³ This raises concerns under Article 26 of the ICCPR (the general non-discrimination norm) and Article 14 of the ECHR, as well as under the specific non-discrimination treaties including the International Convention on the Elimination of All Forms of Racial Discrimination. The OHCHR has specifically called attention to the discriminatory dimensions of surveillance capitalism, noting that the commercial harvesting of personal data and the construction of behavioral profiles tend to entrench and exacerbate social inequalities, as individuals from lower-income and marginalized communities face the most aggressive data exploitation with the least legal recourse.⁶⁴

6. Emerging Challenges: Mass Surveillance, Surveillance Capitalism, and Artificial Intelligence

Mass Surveillance and the Architecture of Bulk Collection

The Snowden revelations confirmed what critical surveillance scholars had long argued: that the normative framework of targeted surveillance predicated on prior judicial authorization of specifically identified targets had been rendered obsolete by bulk collection technologies that intercept all communications and sort them algorithmically.⁶⁵ The distinction between the collection of data and its examination which States invoked to deny that bulk interception constituted an interference with privacy was rejected by the ECtHR in *Big Brother Watch*, which held that the very existence of mass surveillance legislation gives rise to a threat of surveillance affecting all users of electronic communications.⁶⁶ The legal challenge to bulk surveillance is compounded by a transparency deficit: classification of surveillance programmes means that the individuals whose rights are affected cannot know whether they have been subjected to surveillance, and therefore cannot mount effective legal challenges. The OHCHR has called for enhanced transparency reporting by States and technology companies as a minimum accountability measure.⁶⁷

Surveillance Capitalism and Private Sector Obligations

Zuboff's concept of surveillance capitalism captures a dimension of the surveillance problem that is distinct from, though related to, State surveillance: the systematic exploitation of personal data by commercial platforms for the purpose of generating behavioural prediction products sold to advertisers and others.⁶⁸ This form of surveillance is technically lawful in many jurisdictions, yet constitutes a profound interference with individual autonomy and the right to informational self-determination.⁶⁹ The UN framework of business and human rights embodied in the UN Guiding Principles on Business and

⁵⁸ Human Rights Committee, General Comment No. 25, *Participation in Public Affairs and the Right to Vote* (CCPR/C/21/Rev.1/Add.7, 1996).

⁵⁹ Ibid.

⁶⁰ Joseph Cannataci, *Reports of the UN Special Rapporteur on the Right to Privacy to the Human Rights Council and General Assembly*.

⁶¹ Office of the United Nations High Commissioner for Human Rights, *Reports on Privacy, Surveillance, and Human Rights in the Digital Age*.

⁶² Forbidden Stories and Amnesty International, *The Pegasus Project Investigations* (2021).

⁶³ Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) *Proceedings of Machine Learning Research* 1, 7–9.

⁶⁴ OHCHR, *A human rights-based approach to data: leaving no one behind* (OHCHR, 2018) 14–17.

⁶⁵ Surveillance Studies Network, *A Report on the Surveillance Society* (Information Commissioner's Office, 2006) 4; David Lyon, *Surveillance Studies: An Overview* (Polity Press, 2007) 13.

⁶⁶ *Big Brother Watch and Others v United Kingdom* (n 21) para 384.

⁶⁷ Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* UN Doc A/HRC/27/37 (30 June 2014) paras 37–40, 66–67.

⁶⁸ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

⁶⁹ Ibid.

Human Rights (2011) provides an applicable normative framework: corporations have a responsibility to respect human rights, including the right to privacy, and to provide remediation where their operations cause harm. However, the voluntary character of the Guiding Principles limits their effectiveness against powerful technology corporations whose surveillance practices are embedded in their core business models.⁷⁰ The EU General Data Protection Regulation (GDPR) represents the most comprehensive legislative attempt to impose legally binding obligations on private data processors, establishing principles of data minimization, purpose limitation, and privacy by design.⁷¹ The GDPR has influenced data protection legislation across numerous jurisdictions and has contributed to the emergence of what some scholars describe as a global data protection convergence, though significant gaps remain, particularly in the United States and in States of the Global South.

Artificial Intelligence-Enabled Surveillance

The deployment of artificial intelligence technologies in surveillance - including facial recognition, predictive analytics, natural language processing of intercepted communications, and social credit-style scoring systems - presents qualitatively new challenges to the right to privacy and associated rights.⁷² The UN High Commissioner for Human Rights, in her 2021 report on artificial intelligence and human rights, called for a moratorium on AI applications that pose unacceptable risks to human rights, including real-time biometric recognition in public spaces and predictive policing systems.⁷³ AI-enabled surveillance compounds existing concerns about legality, proportionality, and non-discrimination: algorithmic decision-making processes are often opaque, resistant to external audit, and shown to be systematically biased against protected groups.⁷⁴ Facial recognition technology has attracted particular scrutiny. Studies by Buolamwini and Gebru have demonstrated that commercially deployed facial recognition systems exhibit significant accuracy disparities along lines of race and gender, with error rates for darker-skinned women many times higher than for lighter-skinned men.⁷⁵ The European Parliament has called for a ban on facial recognition in public spaces pending the development of an adequate regulatory framework.⁷⁶ The EU Artificial Intelligence Act, which entered into force in August 2024, prohibits the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, subject to narrow exceptions, representing the most far-reaching legislative restriction on AI-enabled surveillance adopted by any major jurisdiction.⁷⁷

The Role of Customary International Law

A question of growing significance is whether the prohibition of arbitrary surveillance has crystallised into a norm of customary international law, binding even on States that are not parties to relevant treaties. The repeated affirmation of the right to privacy in the digital age by UN General Assembly resolutions including A/RES/68/167 (2013), A/RES/71/199 (2016), and A/RES/73/179 (2018)⁷⁸ has been cited by some scholars as evidence of State practice and *opinio juris* supporting such a crystallization.⁷⁹ While the position remains contested, there is growing recognition that the most fundamental aspects of the legality-necessity-proportionality framework for surveillance represent an expression of customary international human rights law. The Special Rapporteur on the Right to Privacy has argued that minimum standards for the oversight and control of surveillance including independent judicial authorization, proportionality assessment, and effective remedies have acquired sufficient normative authority to bind States as a matter of general international law, regardless of treaty membership.

7. Conclusion and Recommendations

The twenty-first century is a human rights challenge in which one of the defining issues is digital surveillance. The normative underpinning of international human rights law, based on Article 17 of ICCPR and Article 28 of ECHR, developed through a body of treaty body general comments, reports of special rapporteurs and a well-established jurisprudence of the ECtHR and CJEU, is adequate for the regulation of digital surveillance. If properly applied, the three-part test of legality, necessity, and proportionality can also restrict the most egregious forms of surveillance. But the divide between the norm and practice is stark. As revealed by Snowden, these mass surveillance programmes are systematic violations of proportionality standards. Under the guise of consent, commercial surveillance capitalism harvests behavioural data from billions of people, which is, in reality, fake. AI enables the expansion of State surveillance and surveillance by

⁷⁰ Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework* UN Doc A/HRC/17/31 (21 March 2011). See also; John G Ruggie, *Just Business: Multinational Corporations and Human Rights* (WW Norton & Company 2013).

⁷¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation) [2016] OJ L119/1 (GDPR), arts 5, 25, 32.

⁷² UN High Commissioner for Human Rights Michelle Bachelet, *Report: Artificial Intelligence and Human Rights*, UN Doc A/HRC/48/31 (3 September 2021) para 7.

⁷³ *Ibid* para 36.

⁷⁴ *Ibid*.

⁷⁵ Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1.

⁷⁶ European Parliament, *Resolution on the use of artificial intelligence in criminal justice and its impact on justice systems*, P9_TA (2021)0016 (European Parliament, 12 February 2021) para 14.

⁷⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) [2024] OJ L2024/1689, arts 5(1)(h), 26.

⁷⁸ UN General Assembly, *The right to privacy in the digital age*, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly, *The right to privacy in the digital age*, UN Doc A/RES/73/179 (17 December 2018).

⁷⁹ James Crawford (ed), *Brownlie's Principles of Public International Law* (9th edn, Oxford University Press, 2019) 594–595.

private actors, which automates violations of privacy on a vast scale and brings new forms of discriminatory impact. AI creates new forms of discriminatory impact and enables the expansion of State surveillance and surveillance by private actors, which automates violations of privacy on a vast scale. International human rights law on this issue moves in three directions of development and recommendations.

First, the progressive development of the understanding of privacy norms by the treaty bodies and regional courts must continue to cover all aspects of the digital world, such as metadata, bulk collection, and AI-assisted surveillance as developed by the ECtHR in the Grand Chamber decision in *Big Brother Watch* and CJEU in *Digital Rights Ireland* and its followers.

Second, the extraterritorial application of privacy norms must be strengthened by the pronouncements of authoritative treaty bodies and State practice, so that intelligence agencies are not able to argue for an exception to the universal nature of human rights based on the nature or location of the information.

Third, most basic of all, there must be institutional innovation in the governance of digital surveillance. The resolution of the Human Rights Council on the protection of human rights on the Internet must be implemented through binding international standards, strong and effective national supervisory bodies with true independence, transparency in the reporting obligations and a moratorium on the most dangerous applications of AI in the field of human rights surveillance, alongside effective remedies for the people whose rights have been violated. Right to privacy is not a legal curiosity that can be left as such: it is the precondition of the exercise of all other rights, of human autonomy and of the possibility of democratic participation.