JOURNAL OF CYBER COVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 8

Spyware Regulation and Proprietary Technology Ownership: Studying Legal Gaps in Cyber Governance Ethics

Mahi Arora

University of Delhi

Recommended Citation:

Arora (2026) "Spyware Regulation and Proprietary Technology Ownership: Studying Legal Gaps in Cyber Governance Ethics" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 8. (DOI)

ABSTRACT

The way modern technologies have evolved over time has significantly changed surveillance practices. The deployment of sophisticated spyware has enabled the government and private entities to monitor the communications and digital activities of the people. The use of spyware by the state is often justified on the grounds of national security, law enforcement, and counter-terrorism, whereas technology is private property; companies that develop such spyware tools keep control over it. The increasing commercialisation and proprietary ownership of such tools raise serious legal and ethical concerns, which are often overlooked. There exists a conflict between the protection of intellectual property rights of technology developers and the safeguarding of fundamental rights such as privacy, data protection and state responsibility.

This paper examines key legal gaps that exist in cyber governance frameworks and challenges posed by spyware and proprietary technology ownership. It explores how legal ambiguities are exploited by the entities under the cover of Intellectual Property (IP) and trade secrets to evade accountability, transparency and state responsibility, arguing for better regulatory oversight and clearer accountability standards for addressing cross-border cyber surveillance and development of comprehensive norms that ensure ethical and responsible governance of spyware technologies.

KEYWORDS

Spyware, Proprietary Ownership, Cyber Governance, Fundamental Rights, Surveillance

INTRODUCTION

Despite the many advantages offered by the advancement of digital technology, it has also led to substantial concerns surrounding data privacy and cybersecurity. Advanced surveillance tools have emerged, which have further intensified the concerns. Over the years, the misuse of spyware has resulted in violations of human rights. Numerous high-profile incidents have been recorded in countries as varied as Greece, Mexico, and Kazakhstan. According to a 2023 intelligence assessment by the United Kingdom's National Cyber Security Centre, over 80 countries had purchased spyware over the previous decade. In 2016, Apple had to make an emergency update to resolve the vulnerability in the operating system, which was found beyond a controlled environment after a suspicious text was sent to the iPhone of United Arab Emirates dissident Ahmed Mansoor.[1] The NSO Group's Pegasus spyware was used for widespread surveillance of the mobile phones of hundreds of journalists, human rights defenders, and political leaders, which was exposed by Forbidden Stories and Amnesty International in July 2021. It has also been found that Intellexa's Predator software was used to spy on many victims, including journalists, politicians, military officials, business leaders and civil society members[2]. The right to privacy has been established by international human rights law, which bars arbitrary or unlawful infringements on the right, and its primary purpose of granting this right is to ensure the protection of human dignity, individual autonomy, and free expression. Article 21 of the Indian Constitution states, "No person shall be deprived of his life or personal liberty except according to procedure established by law".[3]

The individual's right to privacy can be interfered with only by the authorised authorities, like the legislature, executive bodies, and the judiciary, through lawful orders based on reasonable grounds. Article 17 of the International Covenant on Civil and Political Rights (ICCPR),1966 protects the individual from arbitrary or unlawful interferences with privacy[4]. In India, the

[1] Karwan Mustafa Kareem, A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security, SSRN Electronic Journal, 2024 https://www.researchgate.net/publication/382748602_A_Comprehensive_Analysis_of_Pegasus_Spyware_and_Its_Implications_for_Digital_Privacy_and_Security

[2] Aron Ehrlich, To Catch a Predator: Leak exposes the internal operations of Intellexa's mercenary spyware, Amnesty International, 2025 https://securitylab.amnesty.org/latest/2025/12/intellexa-leaks-predator-spyware-operations-exposed

[3] The Constitution of India, art. 21

[4] Right to Freedom of Opinion and Expression: Threats to Media Posed by Unlawful Targeted Surveillance, 2022

Digital Personal Data Protection (DPDP) Act[5] lays down the difference between the ownership of technology and the ownership of personal data. It recognises the primary owner as the individual to whom the data belongs and who has the right to give, manage, or withdraw consent for its use, whereas the companies that develop software are considered Data Fiduciaries who own the proprietary software or technology, but do not own the personal data collected through it. The rapid and unregulated spread of commercial spyware has become a global policy issue as it results in human rights violations, risks to national security, and other harmful activities. Governments as well as non-governmental organisations have widely recognised this concern.

LITERATURE REVIEW

Recent scholarship has identified the emergence of the multi-billion-dollar mercenary spyware market. Companies are providing surveillance as a service by supplying advanced zero-click exploits that allow devices to be infected without any user interaction[6]. Scholars describe this trend as the privatisation of espionage, as private entities now possess technological capabilities that were earlier limited to elite intelligence agencies. This change has enabled governments with adequate financial resources to access and deploy highly sophisticated tools of surveillance.

A key issue raised in recent research is the manner in which proprietary ownership acts as a barrier to effective oversight. The companies that develop technology classify their source code and exploit deployment mechanisms as confidential trade secrets. Scholars have noted that the black box nature of proprietary software acts as a barrier to independent security assessments and meaningful judicial scrutiny. In cases where spyware is linked to human rights violations, it has been observed that companies tend to rely on contractual confidentiality clauses and intellectual property protections to avoid revealing details like user identity and technical specifications. This creates an accountability gap where the technology developer denies responsibility for how the tool is used, while the state that purchases it limits transparency by relying on the developer's proprietary protections.

https://www.ohchr.org/sites/default/files/documents/issues/expression/cfis/threats-digital-age/csos/2023-01-26/Submission-SR%20freedex-hrc50-Amnesty%20Int.pdf

[5] The Digital Personal Data Protection (DPDP) Act, 2023

[6] Osama Hussien, Usman Butt and Rejwan Bin Sulaiman, Critical Analysis and Countermeasures Tactics and Techniques (TTPs) that targeting civilians: A case study on Pegasus, 2023 https://arxiv.org/abs/2310.00769?utm_source

Scholars argue that existing international frameworks like the Wassenaar Arrangement are ill-equipped to address the challenges posed by digital spyware trade. The United Nations Human Rights Office has described these mechanisms as forms of soft law that depend largely on voluntary compliance and lack enforcement mechanisms. Academic literature has discussed several regulatory shortcomings. One major concern is dual-use ambiguity, where spyware is promoted as a tool that is of great importance for combating terrorism and crime, which allows it to bypass stricter export controls that are applied to military technologies. Another issue is jurisdictional arbitrage, under which companies operate through a network of subsidiaries in surveillance-friendly jurisdictions to avoid restrictive domestic regulations. According to the studies published in the International Journal of Intelligent Systems and Applications in Engineering, it has been emphasised that the rapid pace of technological innovation, mainly in encrypted communication and cloud-based infiltration, is much faster than the legislative formulations, which creates a gap in regulatory frameworks. A burgeoning area of literature has explored the role of platform owners such as Apple, Meta and Google as private regulators. As the state regulation has been slow, these companies use proprietary litigation to sue spyware firms for breach of contract or violation of terms of service to uphold global standards.

The literature consistently associates the unregulated spread of spyware with the weakening of Article 17 of the ICCPR, i.e., the right to privacy. Studies suggest that the mere threat of being targeted by proprietary software creates a chilling effect on journalists, activists and political dissidents. The victims have no legal path for redress as technology is invisible and opaque, which undermines the democratic process by facilitating transnational repression, where states target individuals far beyond their physical borders.

Recent scholarship has proposed several integrated measures to address regulatory gaps. One such suggestion is the adoption of Human Rights Due Diligence (HRDD) requirements and mandatory Know Your Customer (KYC) obligations to make companies legally accountable if their technologies are linked to human rights violations. Another recommendation is stronger transparency mandates where the protection of proprietary rights would be overridden by the public interest in situations that involve unlawful surveillance. Scholars also advocate for technical scaling mechanisms and standardised risk assessment frameworks that can classify spyware according to the degree of its intrusiveness instead of the purpose claimed by developers or vendors.

The prevailing consensus in recent literature is to make a shift towards binding international treaties and a re-evaluation of IP protections, which would help in managing the risks associated with the spyware-for-hire industry.

METHODOLOGY

The doctrinal and qualitative analytical methodology has been adopted to examine the regulatory and ethical challenges associated with the use of spyware and proprietary technology. The study mainly relies on secondary sources of data like academic literature, scholarly articles, legal commentaries, policy documents and international reports related to cyber governance, digital surveillance and data protection laws.

The study examines relevant national and international legal instruments that address privacy, cybersecurity, proprietary technology and digital governance. The study throws light on the relationship between proprietary technology ownership and regulatory accountability, as the most surveillance tools used by the state are developed by private technology firms that treat such systems as confidential proprietary assets.

The research focuses on case studies to highlight the challenges that arise from the use of spyware technologies. In order to determine weaknesses in current cyber governance laws, various surveillance tools are studied. This helps in finding out issues such as transparency, accountability, and oversight in the global surveillance industry. Comparisons of different jurisdictions are done to know about the regulation of surveillance technologies and digital monitoring tools, which highlight inconsistencies and legal gaps that can allow the misuse of spyware. The research aims to identify the regulatory weaknesses and make a contribution to academic and policy discussions on improving cyber governance laws, which is needed to ensure transparency in surveillance practices and stronger protection of fundamental rights in the digital world.

ANALYSIS

The use of cyber-surveillance technologies for authoritarian or oppressive purposes has been debated since the early 2010s. After the Arab Spring, the previously obscure private surveillance

industry came under significant public scrutiny. During this period, there were several Western companies that were implicated in supplying surveillance technologies that were allegedly used to commit human rights violations in certain countries. In Germany, one such case occurred during the removal of Hosni Mubarak, where it was indicated by reports that a UK-based firm, Gamma International and its subsidiary FinFisher had supplied their spyware FinSpy to the Egyptian government, which was used to track human rights activists and identify individuals expressing dissent.[7] FinSpy is covertly installed on targeted devices and enables the monitoring of communications such as calls, messages and data exchanges and is also capable of remotely activating the microphone or camera[8]. Some of the cases that involve network surveillance technologies developed by private companies are Amesys, Trovicor, Blue Coat and Sandvine, which were used in Libya, Bahrain, Syria and Egypt, respectively. Although most of these countries are based in Western countries, the surveillance industry has increasingly attracted firms from other regions in recent years, such as China. Many Chinese surveillance companies have capitalised on the growing global demand for monitoring technology by exporting their surveillance systems not just in authoritarian or semi-authoritarian regimes, but also in liberal democracies[9].

The influence of these firms has led to the adoption of these tools in various parts of Africa and Asia by numerous government clients. In 2007, the US National Security Agency initiated unrestricted mass surveillance known as the Prism Program, which was disclosed in 2013. It was used to target not just US citizens but also all internet users across the globe[10].

The well-known case called the Pegasus Project used the software developed by NSO Group. The software was used to target more than 50,000 phone numbers around the world, which also included many high-profile individuals. The Pegasus used the system of zero clicks, which means that there are no actions required by the users. The device can be infected by a mere email or message that contains a cryptic program that can retrieve itself and can be self-installed.

---

[7] Atul Alexander and Atul Alexander, Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism, 2022 https://www.mdpi.com/2075-471X/11/6/85?utm_source

[8] Julia Glazova, FinSpy: the ultimate spying tool, 2021 https://www.kaspersky.com/blog/finspy-for-windows-macos-linux/42383

[9] Adrian Shahbaz, The Rise of Digital Authoritarianism, Freedom House https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

[10] Rikke Frank Joergensen, Can human rights law bend mass surveillance?, Volume 3, Internet Policy Review, 2014 https://policyreview.info/articles/analysis/can-human-rights-law-bend-mass-surveillance

In 2016, Ahmed Mansoor, who was a human rights activist, received suspicious text messages that contained links that, if clicked, would have granted full control of the iPhone. Spyware on Android devices poses serious threats because it has the ability to penetrate systems and compromise sensitive information. A highly advanced spyware known as Chrysaor malware was discovered in 2017, which adopts a dual strategy to obtain unauthorised access. It first attempts to use aggressive technical methods to exploit system vulnerabilities. If this fails, it shifts to social engineering techniques by disguising itself as legitimate software that tricks users into granting the required permissions. After installation, it blocks system updates to obstruct detection and manipulate the data.[11]

In *Manohar Lal Sharma v. Union of India,*[12] the Supreme Court directed the formation of an independent technical committee to investigate allegations that the Indian government used Pegasus against its citizens. In 2024, in the case of *WhatsApp Inc. v. NSO Group Technologies Ltd*[13], a court in the United States held NSO Group responsible for using Pegasus spyware to hack approximately 1,400 WhatsApp users[14].

The data collected using the mass surveillance tools touches on a spectrum of interconnected rights like rights to speech and expression, the right to assemble, and the right to free movement. But the most directly affected right is " the right to privacy", which is a well-recognised human right globally, and has been embedded in the legislatures of many nations.

Article 17 International Covenant on Civil and Political Rights, 1966 (ICCPR), states "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation, and everyone has the right to the protection of the law against such interference or attacks"[15].

Similar provisions can also be seen under Article 12 of the Universal Declaration of Human Rights, which forms part of the broader International Bill of Human Rights, Article 16 of the Convention on the Rights of the Child and Article 22 of the Convention on the Rights of Persons

---

[11] Chirag Sinha, Unveiling Pegasus: Navigating the Nexus Between Spyware And The Sanctity of Privacy, Volume V, Indian Journal of Law and Legal Research https://3fdef50c-add3-4615-a675-a91741bcb5c0.usrfiles.com/ugd/3fdef5_f751ed2e2210469ab86b995873a81baf.pdf

[12] Manohar Lal Sharma v. Union of India, AIR 2021 SC 5396

[13] WhatsApp Inc. v. NSO Group Technologies Ltd., 472 F. Supp. 3d 649 (N.D. Cal.2020)

[14] Scroll Staff, US court finds Pegasus spyware maker liable for unauthorised surveillance of 1,400 WhatsApp users, 2024 https://scroll.in/latest/1077073/us-court-finds-pegasus-spyware-maker-liable-for-unauthorised-surveillance-of-1400-whatsapp-users

[15] International Covenant on Civil and Political Rights (ICCPR),1966, art 17

with Disabilities. Many regional legal instruments have also recognised privacy as a fundamental right of individuals. The scope of privacy protection was expanded in 1988 with the adoption of General Comment No.16 by the United Nations Human Rights Committee concerning Article 17 of the International Covenant on Civil and Political Rights, which acknowledged emerging concerns related to technological and digital surveillance. It states that "the gathering and holding of personal information on computers, databases and other devices by public authorities or private individuals or bodies must be regulated by law."[16] Such a broadened interpretation of privacy rights is also reflected in the jurisprudence of the European Union. In *MK v. France,*[17] the European Court of Human Rights (ECtHR) observed that the protection of personal data was of fundamental importance for an individual's ability to enjoy the right to respect for private life**.** *Schrems v. Data Protection Commissioner,*[18] the Court held that legislation allowing government authorities a generalised access to the content of electronic communications infringes the essential core of the right to privacy under Article 7 of the Charter of Fundamental Rights of the European Union.

Even though there isn't any express right to privacy in the US Constitution, in cases such as *Eisenstadt* v. *Baird*[19] and *Lawrence* v. *Texas*[20]*,* the American courts have expanded the right to privacy. *Justice K.S. Puttaswamy (Retd) v. Union of India*[21] is a foundational Indian case that established the Right to Privacy as a fundamental right.

The major reason for the emergence of international human rights law is the protection of the individual's rights against the state's arbitrary actions.

The concern about the responsibility of international organisations was raised after the adoption of the Articles on Responsibility of International Organisations in 2011; however, the lack of a clearly established legal obligation and a proper standard for determining the attribution of responsibility to organisations makes it challenging to hold them responsible for breaches of international law. Intellectual property ownership further provides immunity to the organisations from any kind of state control. Even though there have been adverse consequences arising from

[16] UN Human Rights Committee (HRC), CCPR General Comment No. 16
[17] MK v. France (App no 19522/09) ECHR 2013 (ECtHR, 18 April 2013)
[18] Schrems v. Data Protection Commissioner [2015] Case C-362/14, ECLI:EU: C:2015:650
[19] Eisenstadt v. Baird, 405 U.S. 438 (1972)
[20] Lawrence v. Texas, 539 U.S. 558 (2003)
[21] Justice K.S. Puttaswamy (Retd) v. Union of India, (2017) 10 SCC 1

the actions of non-state actors, international law has been state-centric in its framework, which results in limited mechanisms to hold firms accountable for the violation of human rights.

Governments have taken several national and multilateral initiatives. The states participating in the Wassenaar Arrangement introduced new control measures for cyber surveillance technology and intrusion software in 2013. There has been a lot of debate around this, but it has marked one of the first multilateral efforts aimed at directly regulating commercial spyware technologies. The governments of France and the United Kingdom launched the Pall Mall Process to address the proliferation and irresponsible use of commercial cyber intrusion capabilities. The scope of this initiative extends beyond commercial spyware technologies to include a wider range of cyber intrusion tools[22].

The two conferences have been held in London and Paris, which resulted in the adoption of the Pall Mall Declaration and a voluntary Code of Practice for States. The Code of Practice has established practices for the development, facilitation, purchase, transfer, and use of such capabilities, which set out the responsible and irresponsible use of commercial cyber intrusion capabilities. In India, governance of spyware and proprietary surveillance technology is undergoing a shift from outdated statutes to a more consent-focused data protection regime. India does not have a dedicated law for spyware; instead, it is regulated by several acts like the Information Technology (IT) Act[23], the Indian Telegraph Act[24], and the Digital Personal Data Protection (DPDP) Act. Unauthorised access to a computer system is criminalised under Section 43 and Section 66 of the IT Act, 2000, which also includes the introduction of computer contaminants like spyware, whereas Section 69 provides the government with the power to monitor and decrypt information for national security and public order. The Digital Personal Data Protection Act, 2023 and its 2025-26 rules have introduced stronger compliance obligations for private organisations that handle personal data, but still, there is persistence of ethical and legal gaps regarding state accountability.

Many big private sector companies, such as Microsoft and Meta, have issued policy recommendations as their products, services, and platforms are targeted and exploited by commercial spyware, which include measures to increase transparency, develop restrictions on

[22] Sven Herpig and Alexandra Paulus, The Pall Mall Process on Cyber Intrusion Capabilities, Lawfare, 2024 https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities

[23] The Information Technology (IT) Act, 2000

[24] The Indian Telegraph Act, 1885

purchase and use of these technologies by government and partner with civil society to help protect users from being targeted with commercial spyware. In 2025, litigation was used to hold commercial spyware companies accountable for their actions. Apple and WhatsApp had initiated legal actions against the NSO Group for breaching their terms of service. While Apple had eventually withdrawn its lawsuit, WhatsApp's case resulted in a significant legal victory where a U.S. court directed NSO Group to pay nearly $170 million in punitive damages to WhatsApp, but later the amount was reduced to $4 million[25].

The three main challenges that need to be addressed are a lack of transparency in the market for commercial spyware and other intrusion capabilities, increased governance for commercial spyware, and legitimate use cases that need to be more clearly defined and distinguished from unacceptable practices. Until these issues are resolved, initiatives in this area will lead only to superficial changes rather than transformative improvements in governance.

DISCUSSION

In a democratic society, law enforcement and intelligence services should coexist by effectively complying with democratic norms and standards and fundamental rights. The technology firms should strictly adhere to professional ethics and operate within their legal mandates, and should have public accountability. The proliferation of spyware tools has led to a growing distrust in digital technologies as users have become aware of the potential risks associated with surveillance and data breaches. The use of spyware tools by the states has made the surveillance and collection of sensitive data normalised. Governments act not only as purchasers and operators of commercial spyware but also as significant participants throughout the entire lifecycle of these technologies. They function as the jurisdictions where spyware companies are based and developed, which enables them to influence the business and investment environment in significant ways. The responsibility lies with national governments for overseeing their own governmental conduct and the use of spyware technologies, which are sold to foreign entities.

The commercial spyware is used by states for legitimate functions such as law enforcement, intelligence, and national security, which has complicated the efforts of governance and made the

[25] Eduard Kovacs, NSO Ordered to Stop Hacking WhatsApp, but Damages Cut to $4 Million, Securityweek, 2025 https://www.securityweek.com/nso-ordered-to-stop-hacking-whatsapp-but-damages-cut-to-4-million

imposition of absolute bans difficult. This has made it necessary to have a clear distinction between lawful and unlawful uses. The presence of surveillance tools on a large scale may create a sense of fear among individuals, which can lead them to withdraw from certain forms of participation. This can undermine the functioning of democratic societies and restrict individuals' ability to exercise their rights to free speech and assembly. As both states and private companies want to acquire increasingly sophisticated capabilities for surveillance and cyber warfare, this can lead to an escalation of a cyber arms race. This can cause instability and increase the likelihood of conflicts emerging in cyberspace.

Governments and private-sector organisations should work jointly to design and promote technologies that effectively protect confidential data and communications of users against unauthorised surveillance. Data minimisation rules should be encouraged by policymakers whose implementation can minimise the amount of data to be collected, which can help in reducing the risk of abuse of personal information exposed to unauthorised surveillance. The regulatory frameworks need to be updated by the government to address the challenges associated with advanced spyware. It also becomes necessary to have international cooperation and shared regulatory standards to develop legal and policy frameworks that protect privacy and encourage responsible behaviour by both state and private organisations, as digital technologies operate on a global scale and have cross-border implications.

CONCLUSION

There are significant challenges created by spyware technologies that need to be addressed on a global level. The examination of the relationship between spyware regulation and proprietary technology ownership has revealed legal and ethical gaps within the digital world. Surveillance tools are created by private companies, which are used by governments for purposes like national security and law enforcement. But the absence of clear regulatory standards has led to privacy violations, misuse of authority, and the weakening of fundamental rights, whereas companies tend to avoid scrutiny by relying on intellectual property protections, which creates a lack of transparency and accountability. Even though these protections are legitimate for innovation industries, they create a lack of transparency due to which surveillance capabilities are misused.

International institutions must develop a shared responsibility framework in order to effectively regulate the conduct of corporations engaged in the cyber-surveillance industry. It is important to ensure that such mechanisms should not just be state-centric but also focus on civil society organisations and corporate entities. It is essential for governments, private sector entities, and academic institutions to collaborate for the development and adoption of end-to-end encryption to ensure that data remains protected while it's in transit and can only be decrypted by the intended recipient. This approach can reduce the ability of advanced spyware to intercept and monitor sensitive communications. Technologies such as blockchain and distributed ledger systems reduce the risks associated with centralised data collection and monitoring by distributing information across multiple nodes within a decentralised network.

The promotion of anonymisation technologies like Virtual Private Networks (VPNs) and the Tor network can help in strengthening privacy protections by concealing users' online identities and reducing the capacity of advanced spyware to monitor their activities.

In conclusion, to effectively counter the threats posed by advanced spyware requires a multidimensional approach that combines stronger encryption and secure communication systems, increasing public awareness and digital literacy, the advancement of privacy-enhancing technologies, updated legal and regulatory mechanisms and greater international collaboration to develop common norms and standards.