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

Volume 5 | Issue 3 | 2026 Art. 6

Beyond Interception: Pegasus, Privacy, and the Indian Constitution

Shailendar Karthikeyan
Law Student, 5th Year, B.A.,LL.B. (Hons.),
Sastra Deemed University, Tanjore, Tamil Nadu

Vignesh Selvam
Law Student, 5th Year, B.A.,LL.B. (Hons.),
Sastra Deemed University, Tanjore, Tamil Nadu

Recommended Citation
Shailendar Karthikeyan and Vignesh Selvam, *Beyond Interception: Pegasus, Privacy, and the Indian Constitution*, 5 IJHRLR 61-90 (2026).
Available at www.humanrightlawreview.in/current-issues/.

Beyond Interception: Pegasus, Privacy, and the Indian Constitution

ABSTRACT

In July 2021, an international investigative exposé revealed that Pegasus – a sophisticated spyware developed by Israel's NSO Group – had been used to target the phones of journalists, opposition politicians, activists, and other private citizens in India[1]. These revelations sparked a furore in Parliament and the media, raising fundamental questions about the right to privacy, the rule of law, and the unchecked reach of executive surveillance power[2]. The Pegasus scandal posed an acute test for India's constitutional commitment to privacy under Article 21 of the Constitution, as affirmed by the Supreme Court in K.S. Puttaswamy (Retd.) v. Union of India (2017)[3]. In response to public outcry and petitions by alleged victims, the Supreme Court constituted an independent committee under Justice R.V. Raveendran to investigate whether the Government had deployed Pegasus against its own citizens[4]. The episode has since become a crucible for examining the tension between national security and individual rights in India's democracy[5]. This essay analyzes the Pegasus surveillance saga through the lens of Indian constitutional law – focusing on the right to privacy and its concomitant standards of proportionality, due process, and accountability – and situates it in a comparative global context of surveillance jurisprudence[6]. It argues that the executive's use of Pegasus-like spyware without robust legal safeguards amounts to executive overreach, falling foul of constitutional norms, and that urgent reforms are needed to bring India's surveillance practices in line with democratic ideals[7]. In developing this analysis, the paper draws on doctrinal foundations from Puttaswamy, the findings of

[1] *The Pegasus Project*, Amnesty Int'l & Forbidden Stories (July 19, 2021), https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project

[2] See Vindu Goel & Mujib Mashal, India Faces Growing Furor Over Allegations of Snooping on Political Opponents, N.Y. Times (July 20, 2021), https://www.nytimes.com/2021/07/20/world/asia/india-pegasus-nso.html

[3] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India)

[4] Manohar Lal Sharma v. Union of India, Writ Petition (Crl.) No. 314 of 2021, Order dated Oct. 27, 2021 (India)

[5] Gautam Bhatia, Surveillance and the Constitution: A Legal Analysis of the Pegasus Controversy, Indian Const. L. & Pol'y Blog (October 2025), https://indconlawphil.wordpress.com

[6] See generally David Lyon, *Surveillance After Snowden* 1–16 (2015); see also Alan Rozenshtein, Surveillance Intermediaries, 70 Stan. L. Rev. 99 (2018)

[7] Ujwal Kumar Singh, The Executive and Covert Surveillance in India: Pegasus and the Erosion of Democratic Accountability, 58 Econ. & Pol. Wkly. (2022).

the Raveendran Committee, and comparative insights from the United States, Europe, and Israel, ultimately proposing a legal framework to reconcile technological capabilities with the rule of law in a constitutional democracy[8].

KEYWORDS

Pegasus spyware, Right to privacy, Executive surveillance, Judicial oversight, Constitutional proportionality

THE PEGASUS SPYWARE SCANDAL AND INDIA'S SURVEILLANCE REGIME

Pegasus and its Use in India

Pegasus is a military-grade "zero-click" spyware – once installed on a target's smartphone, it can turn the device into a 24-hour surveillance tool by silently extracting messages, eavesdropping through the microphone, activating the camera, and copying data, all without the user's knowledge[9]. Unlike traditional wiretapping, which intercepts communications in transit, Pegasus achieves *endpoint compromise*, effectively seizing control of the entire device[10]. In 2021, a consortium of media organisations disclosed a leaked list of about 50,000 phone numbers worldwide selected for possible Pegasus targeting, including over 300 Indians ranging from prominent opposition leaders and journalists to activists and even court officials[11]. Forensic analyses by Amnesty International's Security Lab confirmed Pegasus infections in multiple devices in India, corroborating the suspicions of unlawful surveillance[12]. The Indian government's response was notably evasive. Officials issued blanket denials of "any illegal interception" and claimed that all electronic surveillance is conducted under due process of law, yet they pointedly refused to confirm or deny the use of Pegasus itself, citing national security secrecy[13]. These non-denials, coupled with the

[8] See generally Yuval Shany, Surveillance and the Right to Privacy Under International Law, 68 Am. J. Comp. L. 317 (2020); Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311 (2012)

[9] Amnesty Int'l Tech. & Rsch. Lab, *Forensic Methodology Report: How to Catch NSO Group's Pegasus*, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/[hereinafter *Amnesty Pegasus Forensics Report*]

[10] Ronen Bergman & Mark Mazzetti, The Battle for the World's Most Powerful Cyberweapon, N.Y. Times (Jan. 28, 2022), https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

[11] *The Pegasus Project: Inside the Spyware Scandal*, Forbidden Stories, https://forbiddenstories.org/case/the-pegasus-project/

[12] *Amnesty Pegasus Forensics Report*, *supra* note 1

[13] Rajeev Chandrasekhar, Pegasus Row: Govt Has Not Engaged in Unlawful

government's stonewalling of any substantive debate in Parliament, heightened concerns of executive impunity and prompted several of the targeted individuals to petition the Supreme Court for an independent inquiry[14]. The Pegasus affair thus exposed a troubling *capability-law mismatch*: cutting-edge spyware technology had outpaced India's antiquated surveillance framework, creating the potential for unchecked executive surveillance that could violate fundamental rights with impunity[15].

Supreme Court Intervention – The Raveendran Committee

Acknowledging the gravity of the allegations, the Supreme Court of India broke from past deference on national security matters and, on October 27, 2021, ordered the creation of a Technical Committee overseen by former Justice R.V. Raveendran to investigate the Pegasus allegations[16]. In an interim judgment accompanying this order, the Court made several significant observations[17]. It underscored that mere incantation of "national security" cannot render the judiciary a mute spectator; the State does not enjoy a *blanket immunity* from judicial review when it invokes national security, especially if constitutional rights are at stake[18]. The Court affirmed that surveillance, if conducted by the State, implicates the fundamental right to privacy and must be justified on constitutional grounds[19]. Reiterating the *Puttaswamy* privacy judgment, it held that any invasion of life or personal liberty by the State must satisfy the triple test of: (1) legality (the existence of a valid law authorizing the intrusion), (2) necessity defined by a legitimate state aim, and (3) proportionality (a rational nexus between the means employed and the aim, ensuring the intrusion is no more than necessary)[20]. Crucially, the Court noted that in a democracy governed by the rule of law, "indiscriminate spying on individuals cannot be allowed except with sufficient statutory safeguards, by following the procedure established by law"[21]. It also recognized the chilling effect surveillance can have on free expression, observing that surveillance of the press

Surveillance, Lok Sabha Debates (July 2021), https://prsindia.org/billtrack/monsoon-session-2021

[14] *Manohar Lal Sharma*, *supra* note 4

[15] Apar Gupta, The Pegasus Revelations and India's Outdated Surveillance Laws, 56 Econ. & Pol. Wkly. 19 (2021); see also Vrinda Bhandari & Ujwala Uppaluri, Constitutionalizing Surveillance Reform in India, 15 Indian J. Const. L. 122 (2021).

[16] *Manohar Lal Sharma*, *supra* note 4

[17] Id.

[18] *Id.* at 5–6

[19] *Id.* at 7

[20] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, (India); see also Gautam Bhatia, *State Surveillance and the Proportionality Standard: Puttaswamy Revisited*, 9 Indian J. Const. L. 142, 151–52 (2020)

[21] *Manohar Lal Sharma*, *supra* note 4, at 11

"could result in self-censorship… impinging upon the freedom of the press and consequently on the freedom of speech," particularly by undermining the protection of journalists' confidential sources[22]. With these principled observations, the Court tasked the Raveendran Committee to determine the facts and also to recommend measures for improving India's laws and procedures on surveillance to better protect citizens' privacy in the digital age[23].

Findings of the Committee

The Raveendran Committee's inquiry marked an unprecedented judicially-supervised audit of executive surveillance practices[24]. In its report submitted in August 2022, the Committee revealed that of 29 mobile devices examined from petitioners and others, *five* showed traces of security breaches or malware[25]. However, even in those cases the forensic evidence was not conclusive that the malware was Pegasus itself, as opposed to some other spyware[26]. The investigation was hampered by a lack of official cooperation – the Committee pointedly noted that the Union Government "*did not cooperate*" with the probe by refusing to provide information or clarity on whether it had obtained and used Pegasus[27]. This lack of cooperation drew an explicit remark from the Chief Justice of India in open court, underscoring the Government's disregard for the judicial process ("*the Centre has not cooperated*" in the inquiry)[28]. The Committee's report, delivered in three parts, included a set of recommendations for legal and policy reform[29]. According to the Court's summary, the Committee recommended updating India's surveillance laws to "protect the right to privacy of citizens and ensure the cyber security of the nation", including suggestions to amend existing laws and to establish better oversight mechanisms[30]. While most of the Committee's factual findings remained under seal, the Supreme Court did make public the third part of the report containing these forward-looking recommendations[31]. The Pegasus case thus ended without a definitive finding that the government had used the spyware,

[22] *Id.* at 13.
[23] Justice R.V. Raveendran Comm. Report, in Supreme Court Registry, Public Interest Litigation File (2022) (India) (summary findings on file with author)
[24] *Manohar Lal Sharma*, *supra* note 4
[25] Justice R.V. Raveendran Comm. Report (Part I), *supra* note 23
[26] Id.
[27] Id at 5-6
[28] Ananthakrishnan G., Pegasus Row: Govt Didn't Cooperate, SC Panel Finds, Indian Express (Aug. 26, 2022), https://indianexpress.com/article/india/pegasus-sc-committee-report-govt-did-not-cooperate-8111070/
[29] Justice R.V. Raveendran Comm. Report (Part III), *supra* note 23.
[30] Id.
[31] Supreme Court Registry Press Summary, Pegasus Technical Comm. Report (Aug. 2022), https://main.sci.gov.in/pdf/Press/26082022_175003.pdf

but the proceedings and Committee report nevertheless confirmed serious gaps in the legal framework and urged reforms[32]. The absence of conclusive proof of Pegasus usage – a result that many observers attributed to the evasiveness of the executive and the technical stealth of the spyware – does not erase the constitutional questions raised by the episode[33]. On the contrary, the controversy illuminated how the mere "*menace of surveillance*" (to borrow the European Court of Human Rights' phrase) can violate rights and chill freedoms even in the absence of adjudicated proof of specific instances[34]. The stage was set for a searching reexamination of India's surveillance laws under the touchstone of the Constitution[35].

PRIVACY AS A FUNDAMENTAL RIGHT: CONSTITUTIONAL DOCTRINE IN INDIA

Evolution of the Right to Privacy under Article 21

Privacy's journey to firm constitutional recognition in India was protracted[36]. In the early decades of the republic, the Supreme Court was reluctant to recognize a general right to privacy[37]. In *Kharak Singh v. State of U.P.* (1963), a case concerning police surveillance of a suspect's home movements, the majority struck down nighttime domiciliary visits as violating "personal liberty" but held that there was no fundamental right to privacy per se under the Constitution[38]. Notably, however, Justice Subba Rao's famous dissent in *Kharak Singh* presciently argued that the Constitution's guarantees of life and personal liberty (Article 21) and free movement (Article 19(1)(d)) imply a right to privacy – "*the right to be let alone,*" borrowing Louis Brandeis's phrase.[39] Over time, this view gained traction. In *Gobind v. State of M.P.* (1975), the Court assumed that privacy is a fundamental right deriving from Article 21's guarantee of dignity and liberty, though it stopped short of a definitive pronouncement and held that such a right could be subject to reasonable restrictions.[40] The watershed moment came with the nine-judge bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which unequivocally affirmed that the Constitution protects an intrinsic right to privacy as an

[32] Vrinda Bhandari & Smriti Parsheera, Pegasus: The Legal Vacuum on Surveillance in India, Hindustan Times (Aug. 29, 2022)
[33] Apar Gupta, *supra* note 15
[34] Szabó & Vissy v. Hungary, App. No. 37138/14, Eur. Ct. H.R. (2016).
[35] Gautam Bhatia *supra* note 5
[36] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* 189–90 (2019).
[37] Id.
[38] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (India).
[39] *Id.* at 1309 (Subba Rao, J., dissenting); see also Louis D. Brandeis & Samuel D. Warren, The Right to Privacy, 4 Harv. L. Rev. 193 (1890)
[40] *Gobind v. State of M.P.*, (1975) 2 SCC 148 (India).

aspect of the right to life and personal liberty under Article 21 (as well as various freedoms in Article 19 and the guarantee of equality in Article 14)[41]. *Puttaswamy* overruled the earlier restrictive dicta and elevated privacy to the status of a fundamental right, co-equal with other cherished rights[42]. The judgments in *Puttaswamy* (spanning several concurring opinions) rooted privacy in principles of individual autonomy and dignity, referencing both Indian values and comparative jurisprudence – from Warren and Brandeis's 1890 Harvard Law Review article on *The Right to Privacy*, to US Supreme Court precedents and international human rights norms.[43] As a result, any infringement of privacy by the State now must pass constitutional muster under the rigorous standards discussed below.

The Proportionality and Legality Tests from Puttaswamy

The most significant contribution of *Puttaswamy* (2017) was to articulate a structured doctrine for evaluating privacy violations[44]. The Court held that no restriction on the right to privacy is permissible unless it satisfies a three-part test: (i) legality – the interfering action must have a basis in law; (ii) a legitimate aim – the law must be motivated by objectives of sufficient importance in a democracy (such as national security, public order, etc.); and (iii) proportionality – there must be a rational nexus between the means adopted and the aim, and the extent of interference must be necessary and proportionate to the need.[45] In elaborating proportionality, many Justices in *Puttaswamy* drew on global jurisprudence (including the European "necessary in a democratic society" standard and Aharon Barak's writings), which typically entail a *four-pronged* proportionality analysis: (1) a suitable means (rational connection), (2) necessity (no less restrictive alternative would suffice), (3) a balance between the harm to the right and the benefit to the aim (proportionality stricto sensu), and (4) the presence of procedural safeguards against abuse.[46] Even prior to *Puttaswamy*, the Supreme Court had insisted that surveillance laws include checks and oversight. In *People's Union for Civil Liberties v. Union of India* (1997) – a case dealing with telephone tapping – the Court, while acknowledging state surveillance powers, read procedural due process requirements into the Telegraph Act, laying down guidelines like mandatory review of

[41] *Puttaswamy*, *supra* note 20

[42] Id. See Chandrachud J's observations

[43] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890); see also *Griswold v. Connecticut*, 381 U.S. 479 (1965); *United Nations Declaration of Human Rights*, Art. 12 (1948); *European Convention on Human Rights*, Art. 8

[44] *Puttaswamy*, *supra* note 20

[45] Id. At 264

[46] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* 131–56 (2012); *Handyside v. United Kingdom*, 24 Eur. Ct. H.R. (ser. A) at 23 (1976)

interception orders by a high-level committee and a finite duration for such orders.[47] *Puttaswamy* constitutionalized and strengthened these principles by placing the weight of fundamental rights behind them.

In sum, after *Puttaswamy*, the Indian State may still conduct surveillance for legitimate purposes (e.g. national security, preventing terrorism), but it must do so under a valid law that contains sufficient safeguards, and the surveillance must meet the tests of necessity and proportionality in each case. Blanket or mass surveillance, or surveillance aimed at illegitimate ends (like quelling political criticism), is anathema to these requirements. It is against this doctrinal backdrop that the Pegasus controversy must be evaluated: does India's existing surveillance regime, and the alleged use of Pegasus within it, satisfy the *Puttaswamy* standards and related constitutional mandates? As the next Part explores, there is a strong argument that it does not[48].

PEGASUS VS. THE LEGAL FRAMEWORK: CAPABILITY–LAW MISMATCH AND CONSTITUTIONAL INFIRMITIES

Statutory Powers of Surveillance in India

India's surveillance activities are principally governed by colonial-era legislation and early 2000s IT laws that predate the advent of modern spyware, creating an evident mismatch between governmental capabilities and governing law.[49] The key statutes are the Indian Telegraph Act, 1885 and the Information Technology Act, 2000. Section 5(2) of the Telegraph Act permits the Government to intercept messages transmitted by telegraph (now interpreted to include telephone communications) on the occurrence of any public emergency or in the interest of public safety, when it is "necessary or expedient" to do so for enumerated purposes – namely, the defense of India, national security, public order, or preventing incitement to an offense.[50] This law, born in the era of the telegraph, envisions discrete interception of communication signals (like tapping a phone line) under exceptional circumstances.[51] The Information Technology Act, 2000 updated the legal toolkit somewhat: Section 69 of the IT Act authorizes government agencies to intercept, monitor, or decrypt "any information" generated, transmitted, received or *stored* in any computer resource, again for certain grounds including sovereignty, security of the state, public order, etc., and subject to procedures and safeguards prescribed by the 2009 IT (Procedure and Safeguards for Interception, Monitoring and Decryption

[47] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301, (India).
[48] Vrinda Bhandari & Smriti Parsheera *supra* note 32
[49] Id.
[50] *Indian Telegraph Act, 1885*, § 5(2), No. 13, Acts of Parliament, 1885 (India).
[51] *Supra* note 47

of Information) Rules.[52] These rules mirror the framework of the Telegraph Act – requiring that any interception be approved by a competent authority (usually the Union or State Home Secretary) and reviewed ex post by a Review Committee of executive officials.[53] Section 69B of the IT Act further allows monitoring of "traffic data" for cybersecurity purposes.[54] Notably, neither law explicitly contemplates something as invasive as spyware that *hacks* a device; they speak in terms of "intercepting" or "monitoring" communications.[55] Government lawyers have argued that even hacking into a phone to collect data would fall under "interception" or "monitoring" of information *"stored in"* a computer device under Section 69.[56] However, this is at best an implied interpretation – there is no express statutory mention authorizing the full remote seizure of a device's functionalities. This ambiguity gives rise to serious questions under the *legality* prong of the privacy test: Is the deployment of Pegasus-like spyware even *authorized* by a "law" in force, as required by Article 21? A law must not only exist but also be adequately precise and circumscribed to prevent arbitrary intrusion.[57] Here, the century-old Telegraph Act and the general wording of the IT Act provide, at most, a tenuous and opaque legal basis for such intrusions, arguably falling short of the kind of clear authorization and limitation that the Constitution demands for privacy-invasive measures.[58]

Device Takeover vs. Interception in Transit

The qualitative difference between Pegasus's "device takeover" and ordinary interception is constitutionally significant.[59] Traditional communication intercepts target specific channels: e.g., listening to phone calls or reading emails, usually with the cooperation of telecom or internet service providers.[60] Pegasus, by contrast, infiltrates the device itself, bypassing service providers and seizing everything – microphone, camera, stored files, messages (including encrypted chats, since it captures keystrokes or screenshots before encryption).[61] In effect, it is akin to a general search of a person's entire house and filing cabinets,

[52] *Information Technology Act, 2000*, § 69, No. 21, Acts of Parliament, 2000 (India); see also *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules*, G.S.R. 780(E), Gazette of India (Oct. 27, 2009).
[53] *Id.* Rules 3–8.
[54] *Information Technology Act, 2000*, § 69B.
[55] Chinmayi Arun, *On Surveillance, India's Legal Framework is Dangerously Outdated*, Hindustan Times (July 20, 2021)
[56] Id.
[57] *Puttaswamy*, *supra* note 20
[58] Apar Gupta, *supra* note 15
[59] Chinmayi Arun, *supra* note 55
[60] Id.
[61] *Amnesty Pegasus Forensics Report*, *supra* note 1

rather than placing a tap on their phone line. This breadth of intrusion triggers heightened scrutiny under the *necessity and proportionality* analysis.[62] Even if one assumes national security or crime prevention is a legitimate aim, the means employed must be necessary and no more intrusive than required.[63] It is hard to imagine that surveilling a target's every movement and conversation via spyware is *always* the least restrictive means – especially in cases like journalists or political opponents, where traditional surveillance or open investigation could suffice. Using Pegasus is like deploying a precision-guided missile where a guard post might have done; it tends toward overkill. Indeed, the Supreme Court's *Pegasus* order warned that even national security needs cannot justify "*indiscriminate*" surveillance.[64] Yet Pegasus, by design, is indiscriminate in the data it scoops up: once a phone is infected, there is typically no technical limitation to confine surveillance to only relevant information.[65] All contents and sensors are compromised. Such a dragnet approach risks being held *disproportionate per se* unless tightly controlled. An instructive analogy can be drawn to the U.S. Supreme Court's reasoning in *Carpenter v. United States* (2018).[66] There, the Court held that acquiring extensive cell phone location records (which provided a detailed chronicle of a person's life) required a warrant, emphasizing that the depth and breadth of information gave law enforcement an "*intimate window into a person's life*" not possible with earlier technologies.[67] Pegasus provides not just a window but a comprehensive panoramic view of an individual's private life. Without stringent prior authorization and minimization, its use would fail the requirement that surveillance be narrowly tailored. The Indian government's reported stand – that "no illegal interception" occurred – implicitly suggests it may have treated any Pegasus use as legal interception under existing law.[68] But if authorities equated hacking a phone with routine wiretap, that conflation is dubious at best. Put simply, an executive decision to deploy Pegasus against an individual would amount to a general warrant in effect, something abhorrent to constitutional democracies since the 18th century.[69] The lack of differentiation in law between intercepting a phone call and infiltrating an entire device is a gaping legal void that Pegasus exploits.[70] It underscores the *capability–law mismatch*: the law authorizes

[62] *Puttaswamy*, *supra* note 20
[63] *Aharon Barak*, *supra* note 46
[64] *Manohar Lal Sharma*, *supra* note 4
[65] Vrinda Bhandari & Smriti Parsheera *supra* note 32
[66] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).
[67] Id.
[68] Al Jazeera, *India Targeted High-Profile Journalists with Pegasus Spyware: Amnesty* (Dec 28,2023) https://www.aljazeera.com/news/2023/12/28/india-targeted-high-profile-journalists-with-pegasus-spyware-amnesty
[69] Laura Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181 (2016).
[70] Chinmayi Arun, *supra* note 55

catching a "message in transit," but Pegasus grabs the entire mailbox and the key to the house.[71] This mismatch means the executive could exercise far greater power than what the law, in its letter and intent, ever contemplated – a classic case of administrative overreach violating the principle of legality.[72]

Absence of Judicial Oversight and Due Process

Another glaring deficiency in India's surveillance regime, thrown into sharp relief by the Pegasus saga, is the complete absence of ex ante judicial oversight.[73] Under both the Telegraph Act and IT Act frameworks, surveillance approval is an executive function: authorization warrants are issued by a Secretary in the executive branch, and the only oversight comes from a Review Committee composed of other executive officials (for central intercepts, the Cabinet Secretary and two other Secretaries)[74]. There is no requirement to obtain a court order or involve a judge at any stage, unlike in the United States, UK, or most Western democracies where surveillance of communications typically requires judicial warrant or approval by an independent tribunal.[75] This executive-centric process raises profound *due process* concerns. From a constitutional standpoint, when the government intrudes on fundamental rights in secret, the usual safeguard of an affected person challenging the action in court is practically unavailable.[76] The *Puttaswamy* Court was cognizant of this risk, noting that privacy infringements by surveillance must be accompanied by "sufficient safeguards" and oversight to prevent abuse.[77] In the Pegasus context, these safeguards were conspicuously lacking. The Government never disclosed whether it sought even internal clearance for each target, and if so, what justification was recorded. The Review Committee mechanism, operating entirely behind closed doors, offers at best a perfunctory check – historically, there is no known instance of the Review Committee striking down an interception order.[78] The Raveendran Committee, in fact, recommended establishing an

[71] Vrinda Bhandari & Smriti Parsheera *supra* note 32
[72] *Puttaswamy*, *supra* note 20
[73] Chinmayi Arun, *supra* note 55
[74] *Indian Telegraph Rules*, Rule 419A, inserted via G.S.R. 193(E), Gazette of India (Mar. 12, 2007); *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules*, Rule 4, G.S.R. 780(E), Gazette of India (Oct. 27, 2009).
[75] *Foreign Intelligence Surveillance Act*, 50 U.S.C. §§ 1801–1885c (USA); *Investigatory Powers Act*, 2016, c. 25 (UK).
[76] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248, (India)
[77] *Puttaswamy*, *supra* note 20
[78] Smriti Parsheera, *Pegasus and the Indian Surveillance Framework*, Vidhi Ctr. for Legal Pol'y Blog (Nov 2020) https://www.smritiparsheera.com/research/privacy-surveillance

independent oversight agency or mechanism to address grievances of illegal surveillance, implicitly recognizing that the current system of departmental self-regulation is inadequate.[79] A core aspect of due process is the right to be heard and to seek redress. In secret surveillance, the subject is deliberately kept unaware; thus, ex post notification and remedy become crucial. European human rights law, for example, considers post-surveillance notice (once it can be safely given) as a vital safeguard that allows individuals to challenge unlawful surveillance.[80] Indian law today provides no such right. A victim of Pegasus would likely never know or be able to prove the intrusion unless a third-party report (like the Pegasus Project) alerted them. This puts fundamental rights in a "catch-22": violations may occur with no practical means to contest them, a scenario the European Court of Human Rights in *Zakharov v. Russia* characterized as making secret surveillance "effectively unchallengeable" without special standing rules.[81] While the Indian Supreme Court in the Pegasus case did grant locus to petitioners to seek an inquiry (thus implicitly relaxing the requirement to prove direct harm, akin to the *Zakharov* court's approach of allowing abstract challenges to surveillance laws), this was an ad hoc solution.[82] Systemically, the lack of independent authorization or robust ex post review of surveillance orders in India presents a structural violation of due process and procedural reasonableness under Articles 14 and 21 of the Constitution. An executive that is judge in its own cause on surveillance matters is anathema to the separation of powers and invites abuse – an invitation seemingly accepted in the Pegasus episode, if the allegations are true.[83]

Executive Overreach and Article 14 – Arbitrary or Discriminatory Surveillance

Beyond privacy and procedure, Pegasus also implicates Article 14 of the Constitution, which guarantees equality before the law and non-arbitrariness in state action.[84] A covert surveillance program targeting people for illegitimate reasons (say, journalists exposing government wrongdoing, political strategists of the opposition, or constitutional functionaries) would be a textbook example of arbitrary state conduct. The leaked Pegasus target list in India included, inter alia, a leading opposition politician (Rahul Gandhi), election strategists, two sitting Union Ministers, a former Election Commissioner, and dozens of

[79] *Manohar Lal Sharma*, *supra* note 4
[80] *Roman Zakharov v. Russia*, App. No. 47143/06, Eur. Ct. H.R. (2015)
[81] Id.
[82] *Manohar Lal Sharma*, *supra* note 4
[83] Vrinda Bhandari & Smriti Parsheera *supra* note 32
[84] *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3, (India)

journalists and human rights defenders.[85] Such a roster is difficult to square with any single legitimate investigative purpose; it suggests surveillance deployed broadly against those who could be sources of political challenge or dissent.[86] If indeed an arm of the executive authorized these infections, it constitutes *selective targeting* with no lawful classification or rational basis – thereby violating Article 14's promise that state power will not be used in a capricious or biased manner.[87] The Supreme Court has long held that Article 14 strikes at arbitrariness in governmental measures, even beyond formal discrimination.[88] An arbitrary invasion of privacy – one not based on discernible legal standards or reasonable grounds – offends both Article 21 and Article 14.[89] The Pegasus controversy hints at surveillance being used as a tool of political intelligence, not just security or law enforcement. If proven, that would exemplify the abuse of power that constitutional norms seek to avert: as Justice Jackson of the U.S. Supreme Court cautioned, the power of surveillance "has no conscience" and "no judgment," and when turned against political opponents it destroys personal liberty on the pretext of security.[90] While India's Supreme Court stopped short of making findings on motive or targeting (given the inconclusive evidence), the *possibility* of such abuse – and the Government's non-cooperation to dispel it – reinforces why stricter legal controls are necessary. In a free society, the choice of whom to surveil cannot be left to the unbounded discretion of the Executive, or else the specter of a "surveillance state" looms, where rule of law yields to rule by decree.[91]

It is measured against constitutional requirements, the use of Pegasus in India (to the extent it occurred) appears ultra vires and unconstitutional on multiple fronts: (1) lack of a clear and specific legal mandate (violating the legality requirement); (2) failure of necessity and proportionality given the blanket nature of device hacking; (3) want of independent oversight and due process (leading to executive excess unchecked by neutral scrutiny); and (4) potential arbitrariness or bad faith in target selection (implicating equality and abuse of power)[92]. The upshot is that India's current surveillance law architecture – designed for a bygone era – is ill-equipped to restrain Pegasus-like operations within constitutional

[85] *Phones of Indian Politicians, Journalists Hacked Using Pegasus*, NDTV (July 19, 2021) https://www.ndtv.com/india-news/40-indian-journalists-targeted-by-pegasus-spyware-their-phones-hacked-report-2489415
[86] *Amnesty Pegasus Forensics Report*, *supra* note 1
[87] *Ajay Hasia v. Khalid Mujib Sehravardi*, (1981) 1 SCC 722
[88] *State of W.B. v. Anwar Ali Sarkar*, AIR 1952 SC 75 (India); see also *Maneka Gandhi supra* note 76
[89] *Puttaswamy*, *supra* note 20
[90] *Robert H. Jackson*, The Supreme Court in the American System of Government 75 (1955).
[91] Vrinda Bhandari & Smriti Parsheera *supra* note 32
[92] *Puttaswamy*, *supra* note 20

bounds. This diagnosis finds support not only in domestic principles but also in global norms, to which we now turn for comparative perspective and possible guiding light for reforms.[93]

COMPARATIVE JURISPRUDENCE ON SURVEILLANCE: GLOBAL LESSONS FOR PRIVACY PROTECTION

United States – Fourth Amendment and Judicial Warrants.

In the United States, government surveillance of communications is constrained by the Fourth Amendment's prohibition on "unreasonable searches and seizures," which generally requires judicial warrants issued upon probable cause.[94] In the landmark case of *Katz v. United States*, 389 U.S. 347 (1967), the U.S. Supreme Court held that wiretapping a telephone booth constituted a search, famously declaring that "the Fourth Amendment protects people, not places,"[95] and that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected". *Katz* thus extended constitutional privacy to communications, dismantling earlier doctrines that had allowed warrantless wiretaps. Today, any electronic surveillance for ordinary law enforcement (e.g. wiretaps, bugs) must be authorized by a judicial warrant under a strict statutory regime (the Omnibus Crime Control and Safe Streets Act, 1968, known as Title III) which imposes heavy procedural safeguards – such as particular description of target and time-limited interception, *ex ante* judicial oversight, and *ex post* inventory notices to surveilled persons in many cases.[96] These requirements reflect a judgement that unchecked surveillance is prone to abuse and that neutral magistrates must serve as gatekeepers. Even in the national security realm, the U.S. introduced the Foreign Intelligence Surveillance Act (FISA) in 1978, establishing a special court (FISC) to review and approve surveillance requests involving foreign intelligence within the U.S., albeit under more permissive standards than criminal warrants.[97] The post-9/11 era saw an expansion of surveillance – including warrantless bulk data collection by the National Security Agency (NSA) – but these programs were met with legal challenges and eventually, reforms. In *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), journalists and lawyers who feared NSA surveillance sued, but the Supreme Court denied standing, finding their alleged injuries too speculative.[98] That ruling highlighted a

[93] *Roman Zakharov supra* note 80
[94] U.S. Const. amend. IV.
[95] *Katz v. United States*, 389 U.S. 347, 351–53 (1967).
[96] *Omnibus Crime Control and Safe Streets Act of 1968*, Pub. L. No. 90-351, §§ 801–804, 82 Stat. 197 (codified at 18 U.S.C. §§ 2510–2523).
[97] *Foreign Intelligence Surveillance Act of 1978*, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801–1885c).
[98] *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013).

recurrent accountability gap: secret programs are hard to challenge in court. However, subsequent leaks by Edward Snowden in 2013 brought to light mass surveillance activities (like bulk collection of telephone metadata) and shifted the legal landscape. The Second Circuit in *ACLU v. Clapper* (2015) found the NSA's bulk telephony metadata program exceeded statutory authorization, and Congress enacted the USA FREEDOM Act (2015) to curtail bulk data collection and increase FISA Court transparency.[99] Most pertinently, the U.S. Supreme Court in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), signaled a willingness to adapt Fourth Amendment doctrine to contemporary digital surveillance: the Court held that accessing 127 days' worth of an individual's cell-site location history from telecom providers required a warrant, rejecting the government's argument that such data were "third-party business records" beyond Fourth Amendment protection.[100] Chief Justice Roberts reasoned that the detailed, encyclopedic information about a person's movements and associations over time "provides an intimate window into a person's life" in a way that triggers reasonable expectations of privacy. By analogy, hacking a smartphone with spyware like Pegasus in order to monitor a person's communications and activities would unquestionably be considered a "search" under the Fourth Amendment – one that could only be carried out lawfully with a particularized warrant supported by probable cause. U.S. law enforcement has indeed grappled with the temptation to use such tools; reports emerged that the FBI procured a version of Pegasus (branded "Phantom") for evaluation, though ultimately the Bureau purportedly decided not to deploy it operationally amid legal and policy concerns.[101] The U.S. Government has since taken a public stance against unchecked spyware: in 2021, the Biden Administration blacklisted NSO Group, placing it on the Commerce Department's export control list for engaging in activities contrary to U.S. foreign policy interests (notably, the human rights abuses by some Pegasus clients).[102] While that move was driven by foreign policy, it underscores the view that Pegasus-type surveillance is antithetical to the rule-of-law values that democracies espouse. The U.S. experience illustrates the importance of independent judicial oversight and specialized legal regimes for surveillance. From FISA courts to congressional intelligence committees, multiple layers of accountability (imperfect though they may be) act as a check on executive surveillance

[99] *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015); *USA FREEDOM Act of 2015*, Pub. L. No. 114-23, 129 Stat. 268.

[100] *Carpenter v. United States supra* note 66

[101] Mark Mazzetti et al., *F.B.I. Bought Israeli Spyware Pegasus but Didn't Use It*, N.Y. Times (Jan. 28, 2022) https://www.nytimes.com/2022/01/28/world/middleeast/israel-pegasus-spyware.html

[102] U.S. Dep't of Commerce, *Commerce Adds NSO Group to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://www.commerce.gov/news

powers. The Indian framework, lacking any analogous judicial input or legislative watchdog, appears archaic by comparison, and this gap bears directly on why something like Pegasus could be misused with little trace.[103]

European Court of Human Rights – Privacy and Proportionality in Surveillance

Across the Atlantic, European jurisprudence has developed strong norms on government surveillance under Article 8 of the European Convention on Human Rights (ECHR), which guarantees the right to respect for private life and correspondence.[104] The touchstone in ECHR analysis is that any secret surveillance measure must be not only necessary in a democratic society (a formulation akin to strict proportionality) but also *"in accordance with law."*[105] The latter phrase has been interpreted to require that domestic law authorizing surveillance be adequately accessible and precise, and that it contain effective safeguards against abuse. In a series of cases since the 1970s, the European Court of Human Rights (ECHR) has fleshed out minimum standards for surveillance laws. In *Klass v. Germany* (1978), the Court accepted the principle of secret surveillance for national security but warned that democratic societies needed to ensure such surveillance was strictly necessary and accompanied by adequate guarantees to prevent abuse.[106] Decades later, in *Roman Zakharov v. Russia*, App. No. 47143/06 (Eur. Ct. H.R. 2015) (Grand Chamber), the ECHR delivered a "blockbuster" judgment invalidating Russia's SORM surveillance system for failing these standards.[107] The Russian law on its face required judicial authorization for intercepts, but the Court found *"serious and systematic deficiencies"* in practice and legislation: surveillance was permitted for an overly broad range of offenses with virtually unfettered discretion for security agencies; there was no sufficient independent oversight; telecom providers had to install equipment that gave agencies direct access; and crucially, targets were not notified even ex post facto, nor was there any effective remedy for unlawful surveillance.[108] The ECHR enumerated a set of essential safeguards that any surveillance regime should have to avoid arbitrariness. These include: clear definitions of the categories of people liable to surveillance and the nature of offenses or threats that justify it; limits on the duration of surveillance; procedures for authorizing the surveillance (preferably judicial or independent administrative oversight); procedures for storing, accessing, examining,

[103] Chinmayi Arun, *supra* note 55
[104] European Convention on Human Rights art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.
[105] *Roman Zakharov supra* note 80
[106] *Klass v. Germany*, App. No. 5029/71, 2 Eur. H.R. Rep. 214, ¶¶ 48–50 (1978).
[107] *Roman Zakharov supra* note 80
[108] Id.

and destroying the collected data; and some form of notification or ex post review so that an individual can challenge the measures, at least when such notification can be made without jeopardizing the purpose of the surveillance. The Russian system failed most of these tests, leading the Court to conclude it *"did not provide adequate safeguards against arbitrariness and the risk of abuse"*, in violation of Article 8. By contrast, in cases involving countries like the United Kingdom, the ECHR has scrutinized and prodded reforms but also acknowledged improvements. In *Big Brother Watch v. United Kingdom* (2021, Grand Chamber), which dealt with the legality of the UK's prior bulk interception regime (exposed by Snowden), the ECHR recognized that bulk interception might be a legitimate technique for national security, but it found the UK's earlier system lacking in some respects (e.g., it did not have robust independent authorization for selecting search terms or sufficient protections for journalist communications).[109] The UK by then had enacted the Investigatory Powers Act 2016 ("IPA 2016"), a sweeping new law that actually codified many safeguards: warrants for interception (including bulk warrants) must be approved through a "double-lock" – signed by a Secretary of State and approved by an independent Judicial Commissioner before taking effect; the law created an Investigatory Powers Commissioner's Office (IPCO) for oversight; and provided for a tribunal (Investigatory Powers Tribunal) where individuals can complain of unlawful surveillance.[110] The Grand Chamber in *Big Brother Watch* took note of these developments and set out principles emphasizing the need for end-to-end safeguards in bulk surveillance: targeting, filtering and searching of intercepted material should involve independent supervision, and there must be a mechanism of notifying individuals after the fact whenever possible. The trajectory in Europe thus shows a clear direction: secret surveillance is deemed a serious interference with fundamental rights and is tolerated only subject to rigorous legal strictures and oversight mechanisms, with independent (preferably judicial) control being a hallmark of a convention-compliant system. If we hold up India's Pegasus situation against those European standards, the deficiencies are stark. Indian law as it stands had none of the independent authorization or ex post notification safeguards that the EHR considers crucial.[111] Indeed, one can analogize that India's framework resembled the struck-down Russian model more than the reformed British one – broad executive discretion, lack of transparency, and no meaningful remedy for victims. The Pegasus case, which revealed the potential for "*generalised surveillance*" of a kind that ECHR

[109] *Big Brother Watch v. United Kingdom*, Apps. Nos. 58170/13, 62322/14, 24960/15, (Eur. Ct. H.R. May 25, 2021) (Grand Chamber).
[110] Investigatory Powers Act 2016, c. 25, §§ 20–24, 227–230 (UK); see also IPCO, https://www.ipco.org.uk/
[111] Chinmayi Arun, *supra* note 55

jurisprudence strongly condemns, indicates that India risks running afoul of international human rights expectations, even if those are not directly binding domestically. The comparative lesson is that India should incorporate robust safeguards – judicial or independent authorisation, clear limits, and review mechanisms – to align with what many democracies and international courts regard as necessary for legitimizing surveillance.

Israel – The Security Perspective and Legal Checks on Spyware

The State of Israel presents an intriguing dual perspective on Pegasus. As the home country of NSO Group, Israel has faced international pressure over export of Pegasus to authoritarian regimes, and domestically it confronted its own surveillance controversy.[112] In early 2022, reports surfaced that the Israeli police had used NSO's spyware against Israeli citizens (including figures in a corruption trial) without proper warrants, sparking public outrage and a governmental inquiry. This prompted calls to reform legal restraints on police hacking[113]. Separately, during the COVID-19 pandemic in 2020, the Israeli government empowered the internal security agency (Shin Bet) to perform cellphone contact tracing of infected persons. The Israeli Supreme Court swiftly intervened in *Ben Meir v. Prime Minister* (2020), holding that such invasive electronic monitoring of civilians by a security agency could not be authorized by mere emergency executive decree and required explicit legislation due to its impact on privacy.[114] The Court effectively blocked continued use of the surveillance program absent a statutory basis, emphasizing that democratic legitimacy demanded parliamentary debate and clear limits on any such surveillance measure. The Knesset did subsequently enact a law to allow limited Shin Bet contact tracing, but with oversight and sunset clauses, illustrating legislative control.[115] Most recently, in November 2024, the Israeli government proposed a controversial "Spyware Law" that would formally authorize police to use spyware (akin to Pegasus) in serious criminal investigations, subject to court approval and certain offense thresholds.[116] The bill, introduced by a hardline minister, met with *fierce opposition* from Israel's Attorney General and civil society, who warned that it posed a grave threat to civil liberties and could be "a step towards

[112] Tomer Ganon, *Exclusive: Israeli Police Used Pegasus Without Warrant on Citizens*, *Calcalist* (Jan. 18, 2022), https://www.calcalistech.com
[113] Isabel Kershner, *Israeli Police Illegally Used Pegasus Spyware on Citizens, Inquiry Finds*, *N.Y. Times* (Aug. 1, 2022), https://www.nytimes.com
[114] HCJ 2109/20 *Ben Meir v. Prime Minister*, ¶¶ 21–28 (Isr. Sup. Ct. Mar. 1, 2020) (holding that Shin Bet cellphone tracking required legislative approval).
[115] Jonathan Lis, *Knesset Passes Law Authorizing Shin Bet Contact Tracing Amid Pandemic*, *Haaretz* (July 7, 2020), https://www.haaretz.com
[116] Stuart Winer, *Government Proposes Law to Authorize Spyware Use by Police*, *Times of Israel* (Nov. 9, 2024), https://www.timesofisrael.com

authoritarianism" if not strictly limited.[117] The preliminary version of the law allowed secret installation of spyware with full device access, but only upon a judge's warrant and only for grave offenses (punishable by at least 10 years).[118] In response to criticism, the government indicated it would revise the bill to include stronger oversight and to perhaps remove the most draconian elements.[119] The Israeli debate is instructive: even a nation with acute security concerns acknowledges that police hacking must be grounded in legislation and hemmed in by judicial supervision, narrowly defined scope, and oversight, or else it endangers democracy itself. For India, which shares the ethos of being a constitutional democracy, the Israeli Supreme Court's insistence on legislative sanction for surveillance and the backlash against unchecked spyware use resonate strongly. Just as Israel realized it needed to update its laws to explicitly deal with spyware (rather than letting police repurpose old wiretap laws arbitrarily), India too must confront the reality that its existing laws do not adequately cover or restrain modern surveillance technologies. Failing to do so risks normalizing what Israeli civil society aptly termed "digital occupation" of citizens' private lives[120] – a phrase used to describe Pegasus's use in monitoring dissent in occupied territories and beyond.

Other Democratic Models – Oversight and Accountability

Numerous other democracies offer similar patterns: legislative and judicial involvement as correctives to executive surveillance power. Germany, for instance, has a stringent legal regime for surveillance – the German Constitutional Court in 2008 recognized a fundamental right to the confidentiality and integrity of information technology systems, striking down a state law that had allowed covert police hacking of computers, and holding that such intrusions require weighty justification and specific safeguards (including independent prior review and limitations to core private data).[121] More recently, in 2020, that court invalidated aspects of the foreign intelligence law for insufficient

[117] Israel Democracy Institute, *Statement Opposing the Spyware Law Draft*, IDI Position Paper (Nov. 10, 2024).
[118] Id.
[119] Nir Hasson, *After Criticism, Israeli Government to Revise Spyware Bill*, *Haaretz* (Nov. 15, 2024).
[120] Amnesty International Israel, *Digital Occupation: NSO's Tools and Palestinian Human Rights*, Research Report (Feb. 2022).
[121] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Feb. 27, 2008, 1 BvR 370/07, para. 203 (Ger.), translated in Bundesverfassungsgericht Press Release No. 22/2008, available at https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2008/bvg08-022.html (recognizing a new fundamental right to the confidentiality and integrity of IT systems and striking down provisions for covert hacking by authorities).

protections of privacy even of non-Germans, underlining that privacy rights "exist against the state in its entirety" and surveillance must have oversight even when directed abroad.[122] The United Kingdom, as noted, overhauled its surveillance law with the IPA 2016 after the European court's censure, putting in place multi-tiered oversight.[123] Canada's laws generally require judicial warrants for intrusive surveillance, and Canada has created a National Security and Intelligence Review Agency to review federal surveillance activities, providing an accountability mechanism.[124] Even countries like Brazil have constitutionally entrenched privacy protections and require judicial authorisation for intercepts[125], and South Africa's courts struck down provisions of a surveillance law for lack of notice to persons and absence of post-surveillance remedies as unconstitutional.[126] The consistent theme is that surveillance, especially high-tech surveillance, is seen as *one of the most intrusive forms of state action*, requiring commensurate safeguards to prevent executive abuse. This reflects a broader understanding articulated by scholars that "surveillance is harmful" not just in the breach of privacy of individuals but in its effect on society – it chills free thought and speech (what Professor Neil Richards terms "*intellectual privacy*"), and it skews power dynamics toward the state, enabling potential blackmail or discrimination. Harvard Law Review's influential article *The Dangers of Surveillance* encapsulated this by arguing that unconstrained surveillance "menaces intellectual privacy and increases the risk of blackmail, coercion, and discrimination," and it called for recognizing surveillance as a substantial harm in constitutional doctrine.[127] Comparatively, India's current surveillance practice – secret

[122] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] May 19, 2020, 1 BvR 2835/17, paras. 167–230 (Ger.), available at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html(invalidating provisions of the Federal Intelligence Service Act for lack of safeguards protecting non-German persons' privacy abroad).

[123] Investigatory Powers Act 2016, c. 25, §§ 23, 263–268 (U.K.); Investigatory Powers Commissioner's Office, https://www.ipco.org.uk/ (last visited Oct. 30, 2025) (detailing U.K.'s "double-lock" system of authorization and independent oversight mechanisms).

[124]Nat'l Sec. & Intelligence Rev. Agency, Annual Report 2021 (Can.), https://nsira-ossnr.gc.ca/en/annual-report-2021/(providing oversight of Canada's federal surveillance and intelligence community).

[125] Constitution of the Federative Republic of Brazil, art. 5(XII), translated in Constitute Project, https://www.constituteproject.org/constitution/Brazil_2017.pdf?lang=en (protecting secrecy of communication); see also Marco Civil da Internet, Law No. 12.965/14 (Braz.).

[126] Amabhungane Ctr. for Investigative Journalism NPC v. Minister of Justice & Correctional Servs., 2021 (3) SA 246 (CC) (S. Afr.) (declaring unconstitutional the lack of notice and post-surveillance remedies under the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002).

[127] eil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1934–42 (2013)

orders by the Executive, no independent vetting, no transparency – is an outlier among peer democracies. It tilts the scales entirely in favor of state power, at the expense of individual liberty and democratic accountability. The Pegasus episode has provided a jolting case study of why this imbalance is unsustainable. Just as other jurisdictions have updated laws (sometimes spurred by scandal or court intervention) to rein in surveillance, India faces a normative imperative to do the same, guided by both its own Constitution and the lessons from these global experiences.

THE DEMOCRATIC STAKES: EXECUTIVE OVERREACH, ACCOUNTABILITY, AND THE RULE OF LAW

The Pegasus scandal lies at the intersection of two fundamental tenets of constitutional governance: the preservation of civil liberties (privacy, speech, equality) and the system of checks and balances that guards against concentration of power.[128] When surveillance tools are deployed without adequate oversight, the result is an accretion of unchecked power in the executive – a classic case of *executive overreach* that threatens democratic accountability.[129] In India, the executive branch historically has enjoyed broad leeway in matters of surveillance, shrouded by official secrecy and often exempted from detailed legislative scrutiny.[130] This has fostered a culture of impunity in which intelligence and law enforcement agencies operate in a legal grey zone, with minimal transparency.[131] Pegasus epitomizes the dangers of this status quo. If reports are accurate that Pegasus was used to monitor political opponents, journalists, and even officials of the judiciary, it indicates a collapse of the distinction between legitimate national security surveillance and illegitimate political espionage.[132] Such misuse of surveillance power undermines the democratic process itself: journalists under watch may hesitate to investigate and report freely, opposition politicians may curtail their communications fearing interception, and citizens at large feel the invisible dampening effect on their speech – the so-called "chilling effect" recognized in jurisprudence.[133] Democracy depends on an informed electorate and the free contestation of ideas; pervasive surveillance corrodes both, breeding self-censorship and fear.[134] The framers of the

(arguing that surveillance should be considered a substantial harm and constitutional doctrine must reflect that reality).

[128] *Puttaswamy*, *supra* note 20

[129] Gautam Bhatia *supra* note 5

[130] Alok Prasanna Kumar, *India's Surveillance Regime: Executive Power Without Oversight*, 6 CONTEXTS CONST. DEMOCRACY 72 (2022).

[131] Vrinda Bhandari & Ujwal Pawar, *The Need for a Surveillance Reform in India*, 15 NUJS L. REV. 23, 30–33 (2022).

[132] *Phones of Indian Politicians, Journalists Hacked Using Pegasus*, NDTV *supra* note 85

[133] *Zubair v. State of NCT of Delhi*, (2022) 10 SCC 475, (India)

[134] Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1937 (2013).

Indian Constitution, having witnessed colonial surveillance practices and the excesses of the Emergency (1975–77) when communication privacy was routinely violated, envisioned a rule-of-law state where power would not be unchecked.[135] The emergency-era judgment in *ADM Jabalpur* (1976) – now universally discredited – had infamously condoned executive detentions without remedy.[136] By contrast, decisions like *Puttaswamy* represent the modern Court's resolve that even in national security or emergencies, "the mere mantra of national security" cannot stifle judicial review or constitutional scrutiny.[137] Indeed, the Pegasus case itself is notable for the Supreme Court's assertion that national security considerations do not entitle the government to "a free pass" whenever it claims secrecy.[138] This principle is crucial: *raison d'état* (reason of state) cannot trump the raison d'être of the Constitution, which is to place limits on state power and protect fundamental rights.[139]

From an accountability perspective, one of the most troubling aspects of Pegasus was the Government's refusal to come clean to a constitutional court.[140] The Union Government filed only a limited affidavit, then cited national security to avoid answering whether it had purchased or used Pegasus.[141] This non-transparent posture effectively attempted to oust any oversight – a stance the Supreme Court rightly rejected by proceeding to form the Raveendran Committee.[142] Yet, the Court's deference in not compelling a full answer (perhaps respecting the Committee process) shows the limits of ex post judicial intervention.[143] If the executive simply stonewalls, it becomes challenging for even the judiciary to unearth the truth in national security matters, absent whistleblower revelations or concrete evidence.[144] This is why systemic safeguards are needed ex ante – before rights are violated – rather than relying solely on courts ex post, when the information asymmetry between state and individual is so vast.[145] Democratic accountability also entails legislative oversight. In many democracies, intelligence agencies report to parliamentary committees.[146] India notably lacks a standing

[135] A.G. Noorani, *The Jabalpur Judgment: Still Haunts*, FRONTLINE (May 2011).
[136] *ADM Jabalpur v. Shivkant Shukla*, (1976) 2 SCC 521 (India).
[137] *Puttaswamy*, *supra* note 20
[138] *Manohar Lal Sharma*, *supra* note 4
[139] Anjana Prakash, *Why Surveillance Laws in India Need a Rethink*, THE WIRE (Feb. 2022), https://thewire.in/law/india-surveillance-laws-rethink
[140] *Manohar Lal Sharma*, *supra* note 4
[141] Id.
[142] Id.
[143] Vrinda Bhandari & Ujwal Pawar *supra* note 131
[144] *Clapper v. Amnesty Int'l USA supra* note 98. Also see *Roman Zakharov supra* note 80
[145] *Puttaswamy*, *supra* note 20
[146] U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee), Final Report, 1976.

parliamentary intelligence committee or any comparable mechanism.[147] Surveillance decisions are confined to the executive domain, and Parliament is typically in the dark (barring the occasional leaked scandal that provokes debate).[148] In the Pegasus aftermath, opposition MPs demanded a parliamentary inquiry, but none was granted; sessions were disrupted with protests, and ultimately the matter was shunted to the Supreme Court.[149] This points to a gap in India's accountability architecture – the legislature has not asserted its role in regulating or supervising surveillance, leaving a crucial check missing.[150] The result is what some scholars describe as "surveillance authoritarianism" creeping into democracies: where formal democratic institutions exist, but unchecked surveillance grants the executive a tool to pre-empt and undermine political opposition and civil society, eroding the substantive quality of democracy.[151] Comparatively, countries that have confronted surveillance scandals (from the U.S. Church Committee in the 1970s to recent inquiries in the EU about Pegasus) have strengthened legislative oversight to rein in the executive.[152] India's challenge is to muster similar political will.

The harm from executive overreach in surveillance is not abstract – it strikes at the heart of the social contract. Citizens cede certain powers to the state for protection, but when the state weaponizes those powers against the very people, trust in government evaporates.[153] The Supreme Court in *Puttaswamy* underscored that privacy is intrinsic to the idea of *dignity* and *freedom*, and without it, other rights become fragile.[154] A citizen constantly watched is not truly free.[155] That is why surveillance has been analogized to a "panopticon" – inducing self-censorship and conformity.[156] In a poignant passage, Justice D.Y. Chandrachud in *Puttaswamy* warned that "*privacy safeguards individual autonomy and recognizes the ability of the individual to control vital aspects of her life. Privacy is the condition on which other freedoms depend*".[157] Executive surveillance overreach thus imperils the very conditions for exercising freedom of speech, thought, and association. It also skews the balance of power: a government that knows every move of its critics can perpetuate itself and blunt accountability measures that come through elections or public

[147] Alok Prasanna Kumar *supra* note 130
[148] *Phones of Indian Politicians, Journalists Hacked Using Pegasus*, NDTV *supra* note 85
[149] Id.
[150] Gautam Bhatia *supra* note 5
[151] *Roman Zakharov supra* note 80. Also see *Big Brother Watch v. United Kingdom supra* note 109
[152] Id.; see also *Investigatory Powers Act 2016*, UK.
[153] Neil Richards, *supra* note 134
[154] *Puttaswamy*, *supra* note 20
[155] Id.
[156] Michel Foucault, *Discipline and Punish: The Birth of the Prison* 195–228 (1975).
[157] *Puttaswamy*, *supra* note 20

discourse.[158] In the long run, this can morph a democracy into an elective autocracy.[159] It is telling that many of Pegasus's confirmed end-users have been authoritarian or illiberal regimes – for example, Saudi Arabia (implicated in surveillance of dissidents and associates of Jamal Khashoggi), Hungary (used against journalists and lawyers), and other regimes where checks and balances are weak.[160] If India is to avoid joining that list, it must reinforce the "guardrails of democracy" in the surveillance context. As Justice Brandeis wisely observed over a century ago, "*the greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding*".[161] Pegasus represents that insidious encroachment through technology – often justified by well-meaning appeals to security, but dangerous if unchecked. The task before India's legal and political institutions is to subject such encroachments to the understanding that constitutionalism provides: by imposing limits, oversight, and consequences for abuse.[162]

STRENGTHENING THE LEGAL FRAMEWORK: PROPOSALS FOR REFORM

The Pegasus episode, while deeply troubling, offers India a crucial opportunity to reform and modernize its surveillance laws to better balance security imperatives with constitutional freedoms. Building on the comparative lessons and the Raveendran Committee's recommendations, this Part outlines a blueprint for legal and institutional reforms to prevent executive overreach and ensure any surveillance occurs under the *rule of law*. The overarching goal is to create a surveillance regime that minimizes abuse, maximizes accountability, and aligns with the proportionality standard mandated by *Puttaswamy*. Key elements of the proposed framework include:

Enact a Comprehensive Surveillance Law with Judicial Safeguards

India needs a dedicated, updated law – perhaps a "Digital Surveillance Regulation Act" – to replace or supplement the Telegraph and IT Acts for governing electronic surveillance. This law should explicitly cover modern techniques like spyware, GPS tracking, computer intrusion, etc., and lay down clear conditions for their use. Critically, it must mandate judicial authorization for any surveillance that goes beyond basic, non-intrusive monitoring. For example, a provision could require that to deploy spyware or conduct any search of a digital device, agencies must

[158] Id.
[159] Steven Levitsky & Daniel Ziblatt, *How Democracies Die* 5–9 (2018).
[160] Amnesty Int'l, *Uncovering the Spyware Scandal*, https://www.amnesty.org/en/latest/research/2021/07/the-pegasus-project/
[161] Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).
[162] *Puttaswamy*, *supra* note 20

obtain a warrant from a High Court judge or a specially designated judicial authority (similar to the FISA Court or the judicial commissioners in the UK). The warrant application should demonstrate probable cause (or a defined standard) that the surveillance is necessary for a specific legitimate aim (like investigating a serious crime or a concrete national security threat) and that less invasive methods have been tried or would be ineffective – embedding the *necessity and subsidiarity* principles in the authorization stage. Introducing a judge into the process serves as a neutral check on the executive's claims, filtering out flimsy or mala fide surveillance requests. This reform alone would dramatically align India with established democracies' practices and satisfy the "procedure established by law" requirement in a substantive sense, by ensuring the procedure is just and fair. A "double-lock" system could also be considered: initial authorization by a senior executive official (e.g. Home Secretary) and compulsory approval by a judge or judicial commissioner. Such dual scrutiny (executive + judicial) marries expertise of agencies with independence of judiciary, and was effective in the UK's IPA 2016 framework.

Clear Criteria and Scope Limitations

The new law should tightly define the offenses or situations where surveillance is permitted. For instance, Pegasus-type spyware might be restricted to counterterrorism or counterintelligence operations involving threats to national security, or to investigate particular serious felonies (such as organized crime) – and even then, only upon a showing that the target is reasonably suspected of involvement in those activities. Fishing expeditions or surveillance of individuals for vague "public order" reasons should be prohibited. Drawing from ECHR jurisprudence, the law must avoid giving authorities an "almost unlimited discretion"; instead it should enumerate categories of eligible targets and predicates. Time limits for any surveillance warrant must be imposed (e.g. 60 or 90 days, renewable only with fresh justification to the judge) to prevent indefinite monitoring. The law should also differentiate levels of intrusion – for example, intercepting communication metadata vs. full device access – and calibrate the approval threshold accordingly. Covert device access might demand a higher burden of proof than a simple phone tap, given its intrusiveness. By codifying such substantive limits, the law would give effect to the *legality* prong of *Puttaswamy*, making clear to all (including the executive and citizens) what is allowed and what crosses the line.

Data Minimization and Use Restrictions

Borrowing principles from data protection laws, any surveillance operation should be required to employ minimization techniques. This

means agencies must limit collection to what is necessary for the purpose and, where that's not possible upfront (as with a broad device compromise), they must filter and segregate data so that irrelevant personal information is not retained or is redacted. For instance, if Pegasus is used to investigate a terrorism suspect, and it incidentally scoops up personal photos or communications unrelated to terrorism, procedures should ensure such data is not examined or is promptly destroyed. There should be strict rules on retention: surveillance-acquired data should be stored only for a limited duration unless it is needed as evidence of a crime or for an ongoing serious security operation. The Raveendran Committee's concern about improving cyber security and preventing abuse of collected data aligns with this – agencies should not amass troves of intimate data without cause. Limiting retention also reduces the risk of function creep, where data gathered for X is later misused for Y. Furthermore, clear use restrictions should be in place: information obtained via surveillance should be admissible in court only if the surveillance was lawfully approved and conducted. This introduces an exclusionary rule by statute, which is currently absent in Indian law. Unlike the U.S., where the Fourth Amendment exclusionary rule disincentivizes illegal searches by disallowing their fruits in court, India's courts have held even illegally obtained evidence might be admissible, which removes a key deterrent to misconduct. A statutory mandate that evidence obtained in violation of the surveillance law cannot be used in any judicial or administrative proceeding would strongly incentivize agencies to follow the rules. It also aligns with a fundamental fairness notion – the state should not benefit from its own wrongdoing.

Enhanced Oversight Mechanisms

In addition to prior judicial review, post hoc oversight is vital. An independent watchdog body – e.g. a renamed and empowered Privacy or Surveillance Commission – could be established to audit surveillance practices. This could be a multi-member commission with at least one judicial or retired judicial member and experts in technology and civil liberties. Its mandate: to conduct periodic audits of surveillance warrants and execution, ensure agencies are complying with minimization and data destruction, and report aggregate information to Parliament. The Commission could have access to agency files (with necessary security clearance) to verify that, for instance, Pegasus has not been used beyond approved warrants or that data acquired is handled properly. While operational details may remain classified, the Commission can publish annual transparency reports giving statistics (e.g. number of warrants, number of individuals surveilled, broad categories of reasons) and flagging concerns if any. This would mirror practices in the UK, where the IPCO produces reports, or in the U.S. where intelligence agencies

now release some data on FISA orders. Additionally, Parliament should create a standing Parliamentary Intelligence and Surveillance Committee comprising cross-party MPs with oversight authority over intelligence agencies and law enforcement surveillance. Such a committee, sworn to secrecy, can be briefed on classified programs and can call officials to account. Its existence itself introduces a layer of democratic oversight currently missing. The aim is to end the siloed secrecy that enabled Pegasus to be procured and (allegedly) used without any outside awareness or consent. If the executive knows that both a judge and a legislative committee are in the loop, reckless or purely political surveillance requests are less likely to even be attempted.

User Notification and Remedies

One reform that directly empowers citizens is to mandate ex post notification of surveillance, once it can be done safely. The law could require that within, say, 90 days of the conclusion of a surveillance operation (or after a fixed period if the operation is prolonged), the affected individual must be informed that they were surveilled, with minimal details (dates and type of surveillance) – unless a court finds that giving notice would jeopardize an ongoing investigation or endanger someone. Even in the latter case, notice could be deferred but not denied indefinitely. This practice exists in some form in U.S. criminal wiretap law (where subjects must be notified after the wiretap period ends) and in many European jurisdictions. Notice serves multiple purposes: it allows the individual to seek legal redress if the surveillance was unlawful, it acts as a restraint on authorities (knowing that their actions might later be scrutinized by the subject and a court), and it provides closure to secret state actions. To complement this, the law should provide a statutory civil remedy – a cause of action for those unlawfully surveilled to claim damages or other relief. The cause of action could be designed to be adjudicated in a special tribunal or designated court to handle sensitive information (similar to the UK's Investigatory Powers Tribunal). Alternatively, the existing Human Rights Commissions could be vested with jurisdiction to investigate complaints of illegal surveillance and award compensation. The Supreme Court has also recognized the concept of "constitutional tort" – compensating victims for state violations of rights (e.g., *Nilabati Behera*'s case on custodial death). An unlawful intrusion by spyware is a fit scenario for such relief. Importantly, the fear of monetary liability and public embarrassment can be a deterrent against abusive surveillance. If tomorrow a journalist can sue the government and potentially win damages for being spied on without cause, officials will think twice before authorizing it. Additionally, there should be criminal penalties for officials who misuse surveillance (for instance, conducting it without required approval or for personal gain). While India's Telegraph Act has

some penal provisions, they are outdated and rarely enforced. A new law could criminalize willful violation of surveillance procedures – analogous to how U.S. law makes certain unauthorized surveillance a felony – to underscore that abuse of such power is a serious offense against the state and the citizen.

Protecting Whistleblowers and Ensuring Transparency

As a corollary to oversight, protections for whistleblowers who expose illegal surveillance should be strengthened. Often the public comes to know of abuse only when an insider risks coming forward (for example, Snowden's revelations). India's Whistle Blower Protection Act (2014) is yet to be operationalized effectively and specifically excludes intelligence agencies from its purview. Amendments could carve in protection for disclosures of illegal surveillance to a competent authority (say the proposed Surveillance Commission or a parliamentary committee). This might encourage lawful internal reporting of any Pegasus-like misuse in the future rather than total reliance on external leaks. Transparency can further be enhanced by mandating periodic declassification of older surveillance records. For instance, after a set number of years, the fact of certain surveillance operations could be made public for historical record, once sensitive details are obsolete. This introduces long-term accountability, akin to how the U.S. declassifies FISA court opinions after a lapse of time. Knowledge that one day the veil will lift can discipline behavior today.

In proposing these reforms, one must acknowledge the pushback likely from the security establishment. Critics may argue that involving judges or increasing disclosure could slow down operations or compromise secrets. But experience from other nations shows that a well-designed system can accommodate secrecy and agility while still upholding rights. For instance, FISA courts act swiftly and almost always in secret, yet their presence ensures a rule-of-law process. Emergency provisions can be built in – e.g., agencies may act in urgent situations without prior warrant but must obtain judicial ratification within a short window or cease the surveillance (such as the "exigent circumstances" exceptions recognized in both U.S. and ECHR law). The key is that such exceptions remain exceptions, not the norm.

Ultimately, these reforms are not about hampering law enforcement or intelligence but about legitimizing their necessary operations in a democracy. Surveillance powers, if exercised under robust oversight and clear law, gain public trust and legal certainty. This, in turn, makes evidence collected more readily admissible and prosecutions more likely to succeed, because courts and juries can be assured the evidence was collected lawfully. It also protects the agencies and officers from

politicized allegations, since an independent record would show they followed due process. Thus, strengthening privacy protections and oversight is a win-win: it guards civil liberties while actually enhancing the credibility and effectiveness of genuine national security efforts. As the Supreme Court observed in its Pegasus order, evolution of technology necessitates evolution of law, and the protection of citizens' rights must keep pace with the State's new capabilities. The above proposals are aimed at achieving that balance. They seek to ensure that *"national security"* and *"lawful surveillance"* are not an oxymoron or a smokescreen in India, but concepts defined and limited by the law and Constitution. Adopting these measures would place India among those nations that responded to the challenge of the digital surveillance age by doubling down on democratic values rather than diluting them.

CONCLUSION

The Pegasus spyware saga has been a constitutional awakening for India. It starkly illustrated how 21st-century surveillance technologies, deployed in a legal void, can threaten the fundamental rights and freedoms of citizens, and by extension, the very fabric of democracy. In grappling with Pegasus, India stands at a crossroads familiar to many democracies: whether to allow security technology to outstrip the rule of law, or to update the rule of law to tame the technology. The Indian Constitution – through Article 21, and as elaborated in *Puttaswamy* – emphatically favors the latter course by demanding that even the most powerful state interests be pursued within constitutional constraints of legality, necessity, and proportionality. The findings of the Supreme Court-appointed Committee and comparative jurisprudence from around the world both converge on the same message: secrecy without accountability is a recipe for executive excess, whereas a framework of controlled, oversight-rich surveillance can safeguard both national security and individual liberty.

In many ways, the debate around Pegasus has reaffirmed the enduring wisdom of the Constitution's framers and great jurists. Over a hundred years ago, Louis Brandeis warned that *"the progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping"* and that every unjustified intrusion by the government upon the privacy of the individual, even if undertaken for expedient ends, exacts a great cost to freedom. The Pegasus era, with its zero-click malware, is a dramatic realization of that warning. Yet, it also offers a chance for course correction. By instituting robust judicial oversight, legislative accountability, and strict adherence to the proportionality standard, India can ensure that the right to privacy – now firmly part of its constitutional firmament – is not rendered illusory by technological stealth. The reforms suggested in this essay, from judicial warrants to an

exclusionary rule and post-surveillance notification, are practical translations of constitutional principles into the surveillance context. They seek to make operational the ringing declaration of *Puttaswamy* that "*the life of the law is not logic, but experience*" – here, the lived experience of how unregulated surveillance imperils rights. The experience of Pegasus calls for a legal response that fortifies the ramparts of privacy and civil liberty.

Finally, the Pegasus controversy situates a broader question: what kind of state does India aspire to be in the digital age? A state that, in Justice Khanna's immortal words during the Emergency, preserves the constitution "even when the drums of security are beating," or one that yields to the temptations of absolute power behind a veil of secrecy? The answer will be determined by whether the lessons of Pegasus are heeded. If the constitutional institutions – the judiciary, legislature, and even the executive in reflective moments – take proactive steps to reform surveillance law, India can turn this crisis into an opportunity, setting an example for the world's largest democracy living up to its constitutional promise in the face of modern challenges. If not, the alternative is a gradual normalization of digital authoritarianism by another name, where rights exist on paper but are easily subverted by technology in practice. The stakes thus extend beyond one spyware scandal; they touch the core of India's commitment to constitutionalism. By reclaiming the primacy of rule of law over surveillance technology, India will affirm that in our democracy, it is the Constitution – not any spyware or state apparatus – that ultimately watches over all.