



THE RIGHT TO PRIVACY IN THE DIGITAL AGE:

Recent Judicial Developments in India

Dr. Manjari Singh¹

I. Introduction

The Supreme Court's nine-judge decision in *K.S. Puttaswamy (Retd.) v. Union of India*² settled, in 2017, the threshold question of whether the Indian Constitution recognises a right to privacy. What this decision could not decide was the operation of such a right within all of the particular contexts generated by the increasing digitisation of Indian society: search decisions that could be searched for indefinitely online, the conditions of bail imposed by means of the use of location tracking software, and message services that use encryption to resist any lawful access. The year 2024 saw all of these questions considered by Indian courts to some extent.

In this article I will consider the judicial responses to the issue of the right to privacy in the digital age as decided by Indian constitutional courts in the period of January to December 2024. This analysis will take place along five separate lines of adjudication: the Electoral Bonds case and the treatment of financial privacy; the ongoing jurisprudence of the 'right to be forgotten', emerging from the Madras High Court, the Supreme Court, and the Delhi High Court; the application of the privacy doctrine to bail conditions of location tracking; the ongoing litigation regarding encryption and intermediary traceability obligations; and the judicial response to the phone-tapping in Telangana. A recurring point of reference throughout is that the Digital Personal Data Protection Act, 2023, though enacted, had not been brought into force during the period under review, a fact that shaped, in material ways, the character of the judicial developments discussed below.

II. The Constitutional Baseline: Puttaswamy and Informational Privacy

Puttaswamy located the right to privacy within Article 21's guarantee of life and personal liberty, treating it as an incident of dignity and autonomy rather than as a freestanding textual entitlement.³ Two features of that judgment recur throughout the case law examined in this article. The first is the proportionality standard: any intrusion on privacy by the State must be backed by law, must pursue a legitimate aim, must be necessary, and must be proportionate to that aim. Courts examining privacy claims in 2024, whether in the context of electoral funding, bail conditions, or search-engine indexing, applied some version of this standard, whether explicitly or by clear implication. The second is Justice Kaul's concurring opinion, which recognised, in more limited terms, an individual's interest in controlling the further dissemination of personal information once it enters the public domain, an observation that subsequently developed into the more expansive 'right to be forgotten' doctrine that occupied several High Courts through much of 2024.⁴ The proportionality framework articulated in Puttaswamy, originally formulated in the context of biometric identification and state surveillance, proved sufficiently adaptable in 2024 to be applied to campaign-finance anonymity, bail conditions, and intermediary regulation alike.

III. The Statutory Backdrop: An Enacted but Unimplemented Framework

¹ Assistant Professor, Maneklal Nanavati Law College, Ahmedabad, Gujarat, India.

Email: manjari86singh@gmail.com

² *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

³ *Id.* at ¶¶ 3, 17 (Chandrachud, J.) (locating informational privacy and the right to control dissemination of personal data within Article 21); *id.* ¶ 626 (Kaul, J., concurring) (recognising the right to be forgotten as a facet of privacy).

⁴ Medha Garg, *The Indian Puttaswamy Judgments: Privacy Rights at Stake in the Pursuit of Social Security*, Oxford Hum. Rts. Hub (Apr. 5, 2024).



Parliament enacted the Digital Personal Data Protection Act, 2023 in August of that year.⁵ The Act establishes a consent-based framework for the processing of personal data by data fiduciaries and creates a Data Protection Board of India to adjudicate related disputes.⁶ Throughout 2024, however, the Act remained un-notified. The Ministry of Electronics and Information Technology indicated in July 2024 that draft rules would be released for public consultation only later that year, meaning the statute's substantive obligations had not taken effect during the period under review.⁷

This is a significant contextual fact for the purposes of this article. In the absence of an operative statutory scheme, digital privacy disputes reaching Indian courts in 2024 continued to be adjudicated under Article 21 as elaborated in *Puttaswamy*, supplemented by the residual provisions of the Information Technology Act, 2000 and its 2011 Rules.⁸ The judiciary, in effect, discharged through case-by-case constitutional adjudication a regulatory function that a fully operational data-protection statute might otherwise have performed.

IV. Financial Privacy, Transparency, and the Electoral Bonds Verdict

The Electoral Bonds judgment merits inclusion in this survey precisely because it declined to uphold the privacy claim before it. On 15 February 2024, a five-judge Constitution Bench led by Chief Justice D.Y. Chandrachud struck down the Electoral Bonds Scheme of 2018 in *Association for Democratic Reforms v. Union of India*.⁹ The Scheme had permitted individuals and companies to purchase interest-free bonds from the State Bank of India and transfer them to political parties without disclosure of the donor's identity to the public.¹⁰ The petitioners contended that this anonymity undermined the voter's right to information, itself derived from the freedom of speech and expression guaranteed under Article 19(1)(a). The Union's defence of the Scheme was framed explicitly in the language of privacy: donors, it was argued, possessed a legitimate interest in confidentiality, particularly as a safeguard against political retaliation.¹¹

The Bench rejected this justification. Applying a structured proportionality analysis, it held that whatever privacy interest a donor might claim in remaining anonymous could not outweigh the harm arising from unlimited and untraceable corporate financing of political parties, particularly given the demonstrated correlation between bond purchases and the grant of government contracts and regulatory relief.¹² The Court directed the State Bank of India to furnish complete particulars of every bond purchased since April 2019 to the Election Commission of India for publication, and discontinued the Scheme with immediate effect.

The significance of this decision for the present inquiry lies precisely in its refusal to extend *Puttaswamy*'s protective framework to the claim advanced. It represents one of the clearest instances in the period under review of a constitutional court declining to honour an informational-privacy claim on the ground that the claim, if accepted, would have defeated a competing and, in the Court's assessment, more weighty

⁵Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).

⁶Id. §§ 4-9 (consent, notice, and obligations of data fiduciaries); § 18 (constitution of the Data Protection Board of India).

⁷India's Digital Personal Data Protection Act Rules Set for Public Consultation in August, *Bus. Today* (July 30, 2024).

⁸Information Technology Act, No. 21 of 2000, India Code (2000); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

⁹*Ass'n for Democratic Reforms v. Union of India*, 2024 INSC 113 (India, Feb. 15, 2024).

¹⁰Constitutionality of the Electoral Bond Scheme, *Sup. Ct. Observer* (Mar. 21, 2024).

¹¹Electoral Bonds Held Unconstitutional by Supreme Court, *Lexology* (Mar. 26, 2024).

¹²2024 INSC 113, *supra* note 8, ¶¶ 200-220 (applying the four-fold proportionality standard of *Puttaswamy* and *K.S. Puttaswamy v. Union of India* (Aadhaar), (2019) 1 S.C.C. 1, to the donors' claim of financial privacy).



constitutional value. The decision thereby confirms that privacy under the Indian Constitution, notwithstanding its dignitary foundations, functions as a relational and balanced interest rather than an unconditional entitlement, a proposition that recurs, in varying forms, throughout the remainder of this Article.

V. The Right to Be Forgotten in the Age of Searchable Judgments

No theme occupied Indian courts more consistently in 2024 than the difficulty of reconciling the principle of open justice — that judicial proceedings and judgments constitute public records — with the dignitary interest of individuals, particularly those acquitted or otherwise exonerated, in not remaining permanently identifiable through routine internet search. Three courts addressed this difficulty over the course of the year, and by December 2024 no single, settled standard had emerged.

A. The Madras High Court's Take-Down Order

The controversy originated in *Karthick Theodore v. Registrar General & Ors.* The petitioner, acquitted of a sexual-assault charge in 2011, contended that the continued availability of the judgment on Indian Kanoon, a widely used legal-research platform, had contributed to the denial of an Australian visa application. Rather than confining relief to redaction of identifying particulars, the remedy most courts grant in comparable circumstances, the Madras High Court's order of 27 February 2024 directed that the judgment be removed from Indian Kanoon in its entirety, with only a redacted version permitted for future publication.¹³

B. The Supreme Court's Stay: Publication Versus Redaction

Indian Kanoon appealed the order, and on 24 July 2024 a Bench comprising Chief Justice D.Y. Chandrachud, Justice J.B. Pardiwala, and Justice Manoj Misra stayed the direction of the Madras High Court.¹⁴ The Bench drew a sharp distinction, in its oral observations, between the masking of a victim's or an accused's identity in an appropriate case, a power courts exercise routinely, particularly in matters involving sexual offences, and the wholesale removal of a judgment from a public legal database on the ground that a litigant subsequently found its continued visibility inconvenient. A judgment, the Chief Justice observed, becomes part of the public record upon pronouncement, and a publisher reproducing it faithfully cannot ordinarily be restrained from doing so.¹⁵ The underlying question was however not foreclosed by the Supreme Court of India. It left open, for fuller examination, the extent to which the right to be forgotten permits interference with the public archive of judicial decisions, a reference that remained pending as of December 2024.¹⁶

C. The Delhi High Court's Masking Framework: *ABC v. State*

A more calibrated approach emerged from the Delhi High Court later in the year. In *ABC v. State*,¹⁷ the petitioner had been named as the accused in a matrimonial criminal complaint; the underlying FIR had been quashed by the same High Court in May 2024, yet the case record, including his name, remained fully searchable online. Justice Amit Mahajan held that the right to privacy under Article 21 incorporates a right

¹³MediaNama, SC Stays Madras HC's Right to Be Forgotten Order: Key Points, MediaNama (July 26, 2024) (reproducing the order of the Madras High Court dated Feb. 27, 2024 in *Karthick Theodore v. Registrar General & Ors.*, directing that the 2011 judgment be taken down from Indian Kanoon).

¹⁴*Ikanoon Software Dev. Pvt. Ltd. v. Karthick Theodore*, S.L.P. (C) No. 15311 of 2024 (India, order dated July 24, 2024).

¹⁵Bar & Bench, Right to Be Forgotten: Know the Supreme Court India-Kanoon Case, Bar & Bench (July 24, 2024) (recording the oral observations of Chandrachud, C.J., that a judgment, once delivered, forms part of the public record and that redaction of identifying details in appropriate cases is distinct from wholesale removal).

¹⁶MediaNama, *supra* note 12.

¹⁷*ABC v. State*, 2024 SCC OnLine Del 8113 (Del. H.C., Nov. 6, 2024).



to be forgotten and a right to live with dignity, and that no legitimate public interest was served by perpetuating, through unrestricted internet searchability, the memory of allegations from which the petitioner had been finally absolved.¹⁸ Rather than ordering removal of the judgment itself, the Court directed the Registry to mask the names of both parties, substituting neutral identifiers such as 'ABC' and 'XYZ' in all future pleadings and orders, and permitted the petitioner to approach search engines and other intermediaries to seek de-indexing of identifying material.¹⁹ The reasoning, the legal findings, and the substantive record of the proceedings remained fully intact; only the identifying particulars were suppressed from the public-facing version.

Read together, these three episodes reveal a doctrine still under construction. The Madras High Court's approach of outright removal was, in the Supreme Court's assessment, too blunt an instrument, threatening the integrity of judicial archives and the accountability function that public access to judgments serves. The Delhi High Court's masking framework offers what appears to be a more workable compromise, protecting the dignitary interest underlying the right to be forgotten while preserving the substantive transparency of the judicial record. By December 2024, however, the Supreme Court's own reference remained undecided, and High Courts elsewhere continued to reach divergent results on broadly similar facts, a fragmentation to which this Article returns in Part IX.²⁰

VI. Privacy, Surveillance, and Bail Jurisprudence: Frank Vitus v. Narcotics Control Bureau

A second significant development in 2024 concerned the increasingly common practice, among trial and High Courts, of conditioning bail on an accused sharing a live or pinned location through applications such as Google Maps, so that the investigating agency might monitor the accused's movements. In *Frank Vitus v. Narcotics Control Bureau*,²¹ the appellant, an undertrial in a case under the Narcotics, Drugs and Psychotropic Substances Act, challenged precisely such a condition imposed by the Delhi High Court.

On 8 July 2024, the Supreme Court held that a bail condition enabling continuous, technology-enabled tracking of an accused's movements violates the right to privacy under Article 21.²² The Court's reasoning warrants particular attention. An undertrial, not having been convicted, retains the presumption of innocence and the associated liberty and privacy interests in fuller measure than a convict; bail conditions, accordingly, cannot be fanciful, arbitrary, or freakish, and any restriction on liberty must be no more than is strictly necessary to secure the accused's presence at trial and to prevent interference with the investigation.²³ A condition permitting round-the-clock monitoring of an individual's whereabouts, the Court held, amounts to a form of virtual confinement inconsistent with the very grant of bail, and cannot be justified merely on the ground that the individual retains nominal control over whether to share the

¹⁸Id. (Mahajan, J.) (holding that the right to privacy incorporates the right to be forgotten and the right to live with dignity under Article 21).

¹⁹[Right to be Forgotten] Delhi High Court Directs Masking of Accused's Name in Quashed FIR from Case Records and Online Search Results, SCC Online Blog (Nov. 27, 2024); see also No Public Interest In Keeping Information Alive On Internet After Quashing Of FIR: Delhi High Court On Right To Be Forgotten, LiveLaw (Nov. 22, 2024).

²⁰Compare *ABC v. State*, supra note 16 (Delhi High Court's masking approach), with *Bar & Bench*, supra note 14 (Supreme Court's stay of the Madras High Court's complete take-down order), illustrating the absence, as of December 2024, of a uniform pan-India doctrine on the right to be forgotten.

²¹*Frank Vitus v. Narcotics Control Bureau*, S.L.P. (Crl.) Nos. 6339-40 of 2023 (India, decided July 8, 2024).

²²India: Supreme Court Rules Sharing Google Pin Location as Bail Condition Violates Privacy, DataGuidance (2024).

²³The Intersection of Privacy Rights and Bail: Implications for the Criminal Justice System, Lexology (Oct. 23, 2024); see also From Google Pins to Privacy Wins – Supreme Court Rules Location Tracking Unconstitutional for Bail, Lexology (Sept. 6, 2024).



location.²⁴ The Court further issued notice to Google LLC to ascertain the technical operation of location-sharing on its Maps application, before concluding that the condition served no genuine investigative purpose and ordering its deletion.²⁵

Frank Vitus is significant for extending Puttaswamy's proportionality analysis into the ordinary procedural terrain of criminal bail. It signals to trial and High Courts that surveillance conditions, however administratively convenient for investigating agencies, must be justified with the same rigour as any other State intrusion upon privacy, and that an accused person's formal acceptance of a bail condition does not, without more, cure a disproportionate infringement.

VII. Encrypted Communications and the Limits of State Access: The WhatsApp Traceability Litigation

A third, and as yet unresolved, strand of litigation in 2024 concerns the compatibility of end-to-end encryption with the traceability obligation imposed on significant social media intermediaries by Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.²⁶ That Rule requires such intermediaries, upon a court order or an order issued under Section 69 of the Information Technology Act, 2000, to enable identification of the first originator of a message.²⁷ WhatsApp LLC, whose petition challenging Rule 4(2) had been pending before the Delhi High Court since 2021, continued to press its objections through 2024, contending that compliance is technically impossible without either breaking end-to-end encryption for all users or retaining a permanent, decryptable log of every message transmitted on the platform in India.²⁸

At a hearing on 26 April 2024, before a Bench comprising the Acting Chief Justice and Justice Manmeet Pritam Singh Arora, counsel for WhatsApp submitted that the platform would cease operating in India rather than comply with an order to break encryption, emphasising the reliance placed by hundreds of millions of Indian users on the assurance of private, unreadable communication.²⁹ The Union of India maintained, in response, that no fundamental right, including privacy, is absolute, and that the traceability requirement constitutes a proportionate response to the use of encrypted platforms for the circulation of unlawful content, including material relating to child sexual abuse and communal violence.³⁰ The matter remained sub judice through the close of 2024, with further hearings scheduled, and no final adjudication on the constitutionality of Rule 4(2) had been rendered as of December of that year.³¹

The WhatsApp litigation illustrates a feature of digital-age privacy disputes that distinguishes it from the right-to-be-forgotten cases discussed above. Whereas courts confronting the latter could fashion an intermediate remedy such as masking, encryption presents a more binary technical constraint: a message is either end-to-end encrypted for all users or it is not. The eventual disposal of this litigation will require the Delhi High Court, and in all likelihood the Supreme Court thereafter, to apply Puttaswamy's proportionality

²⁴The Future of Bail Surveillance: Understanding the Implications of the Supreme Court's Stance on Google Pin as a Bail Condition, CALJ Blog (Oct. 6, 2024).

²⁵DataGuidance, *supra* note 21.

²⁶Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), r. 4(2) (Feb. 25, 2021) (India).

²⁷Information Technology Act, 2000, § 69, *supra* note 7.

²⁸WhatsApp LLC v. Union of India, W.P.(C) (Del. H.C.) (petition filed 2021; hearings continued through 2024, next listed Aug. 14, 2024).

²⁹Will Cease to Exist in India if Made to Break Encryption: WhatsApp Tells HC, Bus. Standard (Apr. 26, 2024).

³⁰WhatsApp Tells Delhi High Court It Will 'Exit India' if Forced to Break Encryption, India TV News (Apr. 26, 2024).

³¹Bus. Standard, *supra* note 28.



test to a technological architecture rather than to a discrete administrative or judicial act, a considerably more complex undertaking than the fact-specific balancing exercises examined elsewhere in this Article.

VIII. Executive Surveillance and Accountability: The Telangana Phone-Tapping Investigation

A final development considered in this survey is investigative rather than adjudicatory in character, and is included for the light it casts on the practical gap between constitutional privacy guarantees and the accountability of the surveillance apparatus. Beginning in March 2024, the Hyderabad police arrested a suspended Deputy Superintendent of Police and, subsequently, a retired Deputy Commissioner of Police, in connection with the alleged illegal, large-scale tapping of telephones belonging to politicians, journalists, businessmen, judges, and members of civil society during the tenure of the previous State Government.³² The accused officials were alleged to have operated a dedicated surveillance unit within the State Intelligence Bureau, using leased lines and dedicated systems to monitor targets without lawful authorisation, and to have destroyed electronic records to conceal the operation.³³

While the criminal proceedings arising from these arrests are not, strictly speaking, adjudications on the scope of the right to privacy, the episode occupies an important place in any survey of the year's privacy landscape. It supplies a concrete, contemporaneous illustration of precisely the danger against which Puttaswamy had warned in 2017: unauthorised State, or State-adjacent, surveillance conducted outside any statutory or judicially sanctioned process.³⁴ The bail and anticipatory-bail applications filed by the accused officials through 2024 required courts to weigh the gravity of covert, unauthorised surveillance against ordinary considerations governing pre-trial liberty, reinforcing, at the level of routine criminal procedure, the constitutional seriousness that Puttaswamy had already assigned to unlawful interception.

IX. Cross-Cutting Themes and Critical Assessment

Four observations emerge from the year's case law considered as a whole.

First, proportionality has become the default analytical vocabulary for privacy adjudication in India, deployed with comparable fluency by the Supreme Court in a campaign-finance dispute, a narcotics bail matter, and, albeit implicitly, by the High Courts in right-to-be-forgotten litigation.³⁵ This doctrinal convergence represents a genuine achievement of Puttaswamy's legacy, though it also places considerable strain on trial and High Courts, which must apply an admittedly open-textured standard without the benefit of a comprehensive data-protection statute to structure the inquiry.

Second, the right to be forgotten remained, throughout 2024, the least settled area of privacy doctrine. The Madras High Court's take-down order, the Supreme Court's stay and consequent emphasis on the integrity of public judicial records, and the Delhi High Court's masking framework reflect three distinct institutional instincts, protective, custodial, and calibrative, respectively, and the Supreme Court's own reference on the question remained pending at year's end.³⁶ A litigant seeking analogous relief in a different High Court in December 2024 could not, accordingly, point to a single settled test.

³²Deccan Herald, Phone Tapping Case: Ex-DCP Arrested in Hyderabad, Deccan Herald (Mar. 2024); Telangana: Union Tourism Minister G. Kishan Reddy Demands Judicial Probe into Phone Tapping Case Involving SIB Officials, All India Radio News (Mar. 26, 2024).

³³Telangana EX-DCP Held in Snooping Row Now Faces Abduction and Extortion Case, Indian Express (Apr. 11, 2024).

³⁴K.S. Puttaswamy, *supra* note 1, ¶ 3(D) (Chandrachud, J.) (cautioning against unauthorised State surveillance as an intrusion upon the core of Article 21).

³⁵2024 INSC 113, *supra* note 8; Frank Vitus, *supra* note 20; ABC v. State, *supra* note 16 (each invoking the proportionality standard first articulated in K.S. Puttaswamy, *supra* note 1).

³⁶See *supra* Part V (discussing the divergent approaches of the Madras High Court, the Supreme Court, and the Delhi High Court to the right to be forgotten).



Third, 2024 confirmed that privacy claims may point in more than one direction. The Electoral Bonds verdict shows a constitutional court declining a privacy claim advanced by economically powerful donors precisely because it threatened democratic transparency, while Frank Vitus and the right-to-be-forgotten cases show the same courts vindicating privacy claims advanced by comparatively vulnerable individuals, undertrials and acquitted persons, against the administrative convenience of the State. The throughline is not an unconditional preference for privacy, but a sustained willingness to interrogate who benefits from a given assertion of privacy, and at whose expense.

Fourth, the continuing non-application of the Digital Personal Data Protection Act, 2023 ensured that the privacy case law of 2024 was overwhelmingly constitutional in nature, as opposed to statutory, and ad hoc rather than systemic. The courts were left to perform, via Article 21, a regulatory role that an actual data-protection legislation and a Data Protection Board should otherwise have played at the very least where informational-privacy claims by private data fiduciaries were concerned. This excluded many areas of digital privacy injury, especially commercial data processing, from being part of the judicial evolution discussed in this Article since there was little statutory foundation for such claims.

X. Conclusion

No single decision rendered between January and December 2024 carries the foundational weight of Puttaswamy. What the year produced instead was a mosaic of incremental rulings: a Constitution Bench subordinating a donor's claim of financial privacy to the electorate's right to know; a Supreme Court prepared to strike down bail conditions that transform judicially sanctioned liberty into technologically enabled confinement; a Madras High Court and a Delhi High Court reaching for different instruments, deletion and masking, respectively, to reconcile digitised judicial transparency with individual dignity, with the Supreme Court's own view still awaited; a Delhi High Court adjudicating, without final resolution, whether encryption itself may be sacrificed to a traceability mandate; and a set of criminal proceedings in Telangana that gave concrete form to Puttaswamy's warning against unchecked surveillance. Taken together, these developments suggest that Indian courts, in the continued absence of an operational statutory data-protection regime, remain the principal institutional site at which the content of digital-age privacy is being determined, proportionality analysis by proportionality analysis. Whether the eventual notification of the Digital Personal Data Protection Act, 2023 will relieve that institutional burden, or merely add a further layer to it, is a question the judicial developments of 2025 and beyond will have to answer.



Bibliography

A. Constitution and Statutes

India Const. art. 19, cl. 1(a).

India Const. art. 21.

Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).

Information Technology Act, No. 21 of 2000, India Code (2000).

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India).

B. Table of Cases

ABC v. State, 2024 SCC OnLine Del 8113 (Del. H.C., Nov. 6, 2024).

Association for Democratic Reforms v. Union of India, 2024 INSC 113 (India, Feb. 15, 2024).

Frank Vitus v. Narcotics Control Bureau, S.L.P. (Crl.) Nos. 6339-40 of 2023 (India, decided July 8, 2024).

Ikanoon Software Development Pvt. Ltd. v. Karthick Theodore, S.L.P. (C) No. 15311 of 2024 (India, order dated July 24, 2024).

Karthick Theodore v. Registrar General & Ors. (Mad. H.C., order dated Feb. 27, 2024) (as discussed in the secondary sources cited in Part V.A infra).

K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

K.S. Puttaswamy v. Union of India (Aadhaar), (2019) 1 S.C.C. 1 (India).

WhatsApp LLC v. Union of India, W.P.(C) (Del. H.C.) (petition filed 2021; pending as of December 2024).

C. Secondary Sources

Bar & Bench, Right to Be Forgotten: Know the Supreme Court India-Kanoon Case, Bar & Bench (July 24, 2024).

Business Standard, Will Cease to Exist in India if Made to Break Encryption: WhatsApp Tells HC, Bus. Standard (Apr. 26, 2024).

Business Today, India's Digital Personal Data Protection Act Rules Set for Public Consultation in August, Bus. Today (July 30, 2024).

Centre for Applied Law and Justice, The Future of Bail Surveillance: Understanding the Implications of the Supreme Court's Stance on Google Pin as a Bail Condition, CALJ Blog (Oct. 6, 2024).

DataGuidance, India: Supreme Court Rules Sharing Google Pin Location as Bail Condition Violates Privacy, DataGuidance (2024).

Deccan Herald, Phone Tapping Case: Ex-DCP Arrested in Hyderabad, Deccan Herald (Mar. 2024).

Indian Express, Telangana EX-DCP Held in Snooping Row Now Faces Abduction and Extortion Case, Indian Express (Apr. 11, 2024).

India TV News, WhatsApp Tells Delhi High Court It Will 'Exit India' if Forced to Break Encryption, India TV News (Apr. 26, 2024).

Lexology, Electoral Bonds Held Unconstitutional by Supreme Court, Lexology (Mar. 26, 2024).

Lexology, From Google Pins to Privacy Wins – Supreme Court Rules Location Tracking Unconstitutional for Bail, Lexology (Sept. 6, 2024).



Lexology, The Intersection of Privacy Rights and Bail: Implications for the Criminal Justice System, Lexology (Oct. 23, 2024).

LiveLaw, No Public Interest In Keeping Information Alive On Internet After Quashing Of FIR: Delhi High Court On Right To Be Forgotten, LiveLaw (Nov. 22, 2024).

Medha Garg, The Indian Puttaswamy Judgments: Privacy Rights at Stake in the Pursuit of Social Security, Oxford Hum. Rts. Hub (Apr. 5, 2024).

MediaNama, SC Stays Madras HC's Right to Be Forgotten Order: Key Points, MediaNama (July 26, 2024).

All India Radio News, Telangana: Union Tourism Minister G. Kishan Reddy Demands Judicial Probe into Phone Tapping Case Involving SIB Officials, News on Air (Mar. 26, 2024).

SCC Online Blog, [Right to be Forgotten] Delhi High Court Directs Masking of Accused's Name in Quashed FIR from Case Records and Online Search Results, SCC Online Blog (Nov. 27, 2024).

Supreme Court Observer, Constitutionality of the Electoral Bond Scheme, SCO (Mar. 21, 2024).