WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Impact of End-to-End Encryption on Digital Evidence Access: A Privacy vs. Public Safety Debate

Shashank Gulia[1], Dr. Anjali Dixit[2]

[1]Student, LL.M. (Master of Laws), SRM School of Law, SRM University, Sonepat, Haryana, India.
[2]Associate Professor, SRM School of Law, SRM University, Sonepat, Haryana, India.

ABSTRACT

This study critically assesses End-to-End Encryption (E2EE) in Indian law concerning digital privacy and access to electronic evidence for law enforcement, bearing in mind the legal, technical, and ethical ramifications. E2EE ensures that only the communicating parties have access to the transmitted content and has thus become synonymous with digital-type privacy and cybersecurity. However, since the very architecture of E2EE is to prevent service providers from decrypting data, it poses serious difficulties in carrying out legitimate investigations, particularly under Section 69 of the Information Technology Act, 2000, and Section 91 of the Bharatiya Nagarik Suraksha Sanhita. Through a comparative legal analysis, the paper points to the growing global difficulties faced in striking a balance between the right to privacy and the imperatives of public safety, with the international human rights instruments, U.S. and EU regulatory framework, and landmark judicial decisions featuring prominently. The "Going Dark" phenomenon—that is, instances when legal authority is thwarted by technological advances—is considered, alongside potential solutions such as key escrow and client-side scanning, both of which are shown to pose new security risks and constitutional challenges. The study suggests that any kind of lawful access regime be narrowly crafted, be proportionate, and be subject to strict judicial oversight. Furthermore, the paper argues for a rights-based, technologically informed legal framework that addresses the investigative need while protecting digital liberties in line with India's constitution and international obligations.

Keywords: End-to-End Encryption, Digital Privacy, Lawful Access, Indian Surveillance Law, Digital Evidence, Going Dark, Constitutional Rights

1. Introduction

This study critically assesses End-to-End Encryption (E2EE) in Indian law concerning digital privacy and access to electronic evidence for law enforcement, bearing in mind the legal, technical, and ethical ramifications. E2EE ensures that only the communicating parties have access to the transmitted content and has thus become synonymous with digital-type privacy and cybersecurity. However, since the very architecture of E2EE is to prevent service providers from decrypting data, it poses serious difficulties in carrying out legitimate investigations, particularly under Section 69 of the Information Technology Act, 2000, and Section 91 of the Bharatiya Nagarik Suraksha Sanhita. Through a comparative legal analysis, the paper points to the growing global difficulties faced in striking a balance between the right to privacy and the imperatives of public safety, with the international human rights instruments, U.S. and EU regulatory framework, and landmark judicial decisions featuring prominently. The "Going Dark" phenomenon—that is, instances when legal authority is thwarted by technological advances—is considered, alongside potential solutions such as key escrow and client-side scanning, both of which are shown to pose new security risks and constitutional challenges. The study suggests that any kind of lawful access regime be narrowly crafted, be proportionate, and be subject to strict judicial oversight. Furthermore, the paper argues for a rights-based, technologically informed legal framework that addresses the investigative need while protecting digital liberties in line with India's constitution and international obligations.[1]

2. Definition and Functioning of End-To-End Encryption

In this era of computers, the communication goes on to shift very fast from being face-to-face and old kinds of letter exchanges to prompt real-time interactions made possible by several online kinds of platforms. A parallel need to develop mechanisms that provide security to digital interactions against unauthorized surveillance and misuse arises. E2EE is an instance of such a mechanism. E2EE, or End-to-End encryption, is strongly adopted - expectedly so for the most part- by criminal defense lawyers, by foreign countries trying to protect their economic and military communications, by privacy groups, by technologists trying to build innovation safeguards against the state's interference, and even by corporate actors trying to hide spoofing from one another. Generally, it will probably be viewed as bad news for law enforcement since it actively prohibits them from investigating and prosecuting serious crime. In the Indian context, the debate gains momentum within the context of striking a balance between constitutional privacy interests and national

[1] Jessica Shurson, "A European Right to End-to-End Encryption?", 55 *CLSR* 187 (2023).

security concerns. The legal framework must have its accommodation for the digital rights as well as the necessities of accessing evidence for the sustenance of justice.

E2EE stands apart from other forms of encryption due to its specific structure and design, which allows communication strictly between the sender and the recipient. During transmission via E2EE, messages get encrypted on the sender's device and decrypted on the receiver's device. No third party including the service provider, the internet service operator, or an intermediary can decrypt or read the content as it is going through the network. In traditional encryption, the service providers usually retain decryption keys and can hence be granted potential access under legal coercion. E2EE has thus become a technical remedy with the explosion of internet-based communications, in order to protect sensitive conversations from illegal interception, which could be business, private, or even journalists' conversations. In India, where breaches and surveillance threats abound, the functioning of encryption like E2EE is key to maintaining people's trust in digital platforms.[2]

The message is made into a complex cipher before leaving the sender's device with an encryption key which is unique and private. The recipient's device, on the other end, with the corresponding decryption key, transforms this ciphered message into a readable one. If ever intercepted during execution, an unrelated party sees just meaningless data. The service providers that facilitated the exchange cannot read or decrypt these messages even if a subpoena comes in, as they do not hold or control the encryption keys: this is why it is called a "trustless" system. A common user would not have to trust a company to uphold the data privacy of their data. E2EE raises a few content questions on compliance with directives for data sharing under "Section 69" of the Act that allow interception by the government in specified circumstances. This is because, by design, the E2EE framework precludes such interception, rendering legal enforcement very difficult unless surveillance laws themselves are reformed.

3. The Rise of Digital Communication and the Need for Privacy

There has been an explosive rise in digital communication in both volume and frequency in the past decade. Social media applications, instant messaging services, and digital collaboration tools have become everyday essentials for the common man and business entities. At the time of digital proliferation, privacy has simultaneously taken helm as a principal issue, as more and more personal, professional, and political content goes through these channels. Given that India is expected to cross 900 million internet users at the end of 2025, the scale of digital communication is indeed staggering. Also, since issues and alerts on data theft, surveillance, and cyberattacks are ever-rising, the demand for robust privacy mechanisms such as E2EE has exponentially risen. Privacy is more than just a preferred issue for the user; it has been held as a fundamental right under "Article 21 of the Constitution of India", as seen in the judgment of "*Justice K.S. Puttaswamy v. Union of India*"[3] E2EE stands on that constitutional decree by keeping communications private and secure from unauthorized intrusion. But the same aspect that protects individual liberties also creates a burden for law enforcement and judicial systems when they have to gather evidence.

1.1.1. Statistics on Digital Communication Growth, Such as the Billions of Daily Messages Sent Via Encrypted Apps Like Whatsapp and Telegram

The entire last decade has observed the explosive evolution of digital communication. In a 21st-century society, social media applications, messaging applications, and digital collaboration tools are daily requirements. In the wake of digital proliferation, the importance of privacy has been considerably magnified, as now much information of these channels is being processed-information personal, professional, and political. These fast-paced channels of communication happen to build and multiply digital mass. Countries like India are projecting their internet users to cross 900 million by the end of 2025, which shows some magnitude of digital communication in this country. The growing concern of identity theft, surveillance, or cyberattacks requiring stronger privacy: E2E is one. Privacy is not just a lose-their-preference approach with The Supreme Court of India considering privacy as a fundamental right under Article 21 itself in *Justice K.S. Puttaswamy v. Union of India*[4]. E2EE safeguards the very constitutional mandate for private communication from unlawful intrusion. However, the very attribute that assures individual freedoms obstructs in retrieving evidence for law enforcement and judicial setups.

1.1.2. Importance of Privacy in Protecting Against Cyber Threats, Government Surveillance, and Data Breaches, Emphasizing E2ee's Role in Securing Sensitive Information

Privacy implies maintaining users' autonomy; unlike many other human rights, it supports the establishment of trust in the digital environment. Without privacy, users remain vulnerable to identity theft, fraud, phishing, and illegal forms of surveillance. E2EE protects sensitive information related to medical history, financial transactions, political opinions, and personal conversations from being exploited. In India, where awareness about digital safety is still evolving and cybercrime countermeasures are lacking, this protection holds greater significance. It also forms a defence against mass surveillance by the government. The threat of overmighty surveillance lurks in the shadows with the enactment of laws such as the "Information Technology Act, 2000" and the deposit of powers in the government under "Section 5(2)" of the "Indian Telegraph Act, 1885." Against such powers, E2EE remains an effective tool to maintain user rights. At the same time, such an impenetrable barrier of privacy poses very serious challenges to the security and intelligence agencies,

[2] Gurshabad Grover, Tanaya Rajwade, et.al., "The Ministry and the TRACE: Subverting End-to-End Encryption", 14 *NUJS L Rev* 126 (2021).
[3] (2017) 10 SCC 1.
[4] (2017) 10 SCC 1.

who many times contend that E2EE also protects the wrongdoers engaged in criminal activities. The judiciary must then weigh these competing interests in a manner that does not weaken constitutional protections while not undermining investigative powers.[5]

4. The Challenge: Access to Digital Evidence

While one may argue that privacy needs sacred protection, controversy can very well arise should these schemes be used by bad elements to commit or further their criminal acts. Digital evidence was found to be vital for law enforcement activities and judicial process nowadays. Anything from cyberbullying and fraudulent finance to terrorism and child pornography-there may be a digital trail left by perpetrators by far the most credible evidence. Investigators may use metadata, chat transcripts, call logs, histories of locations, and file transfers to prosecute criminals. But under E2EE, service providers cannot decrypt messages even with a court-issued search warrant. This stalemate has been rising the so-called "Going Dark" scenario according to law enforcement agencies—cases where communications channels remain impenetrable even with legal authorisation. Indian authorities under "Section 91" and "Section 92" of the "Bharatiya Nagarik Suraksha Sanhita" (BNSS), which permit requisitioning of documents and records, are unable to obtain usable evidence from encrypted services. Hence, this lack of access frustrates the ongoing investigation, while prosecution cases in courts of law would be thrown out.

1.1.3. Role of Digital Evidence in Modern Investigations, Including Its Use in Prosecuting Crimes Like Terrorism, Child Exploitation, and Cybercrime

This example perfectly illustrates the battle between privacy and good law enforcement. Whenever criminals use encrypted communication platforms to commit or plan crimes, the fight gets intense. Digital evidence has become an essential aspect of modern law enforcement and judicial procedures. Offenders commit crimes ranging from cyberbullying and financial fraud to terrorism and child pornography, and the digital trail left behind is usually the most reliable evidence. These investigators rely on metadata, chat transcripts, call logs, location history, and file transfers to prosecute offenders. However, in the case of data protected by E2EE, even search warrants issued by a court will not compel service providers to decrypt messages. This stalemate came to be known by law enforcement agencies as the "Going Dark" phenomenon, a situation where communication channels are technically impenetrable even after legal clearance. Indian authorities working under "Section 91" and "Section 92" of the "Bharatiya Nagarik Suraksha Sanhita" (BNSS), which provide for the requisition of documents and records, thus find themselves unable to extract usable evidence from encrypted services. The deprivation of further leads hampers investigations and allows the prosecution to cross-question the credibility of their own case in courts of law in the absence of credible digital evidence.[6]

1.1.4. The "Going Dark" Problem, Where E2ee Prevents Law Enforcement from Accessing Critical Evidence, Even with Legal Authorization, as Noted by the FBI (FBI Lawful Access)

Environments are filled with digital evidence invaluable in the solving of murders in wide criminal domains. Communication channels involving encrypted applications provide terrorism-related chats and media files that play a critical role in deciphering networks, pattern formations, and financial transactions. Child exploitation relies heavily on encryption to circulate such illegal content, arranging shadowed exchanges, and victim targeting. Crimes of the cyber-variety: hacked information, phishing, ransomware attacks, and frauds—all go whispered down the digital spoor through data in devices or cloud and communication records. Investigation agencies face a wall when E2EE protects these communications, and providers themselves have no way to access the decrypted contents. This becomes a great impediment in the very enforcement of legislations such as the "Information Technology Act, 2000", and the "Unlawful Activities (Prevention) Act, 1967." Although Section 100 of the Bharatiya Nyaya Sanhita empowers authorities to enter the premises and conduct a search, they may be powerless to decrypt the content if they lack access to such keys. A serious conundrum is thus drawn forth—discount all instances of encryption in the interest of public safety, or uphold privacy as a premise for compromising any trace of evidence?

The phrase "Going Dark" refers to where law enforcement agencies with judicial authority are constrained from accessing the content of communications owing to technical inability caused by encryption. End-to-End Encryption joins in perpetrating this problem by making sure that service providers cannot even give the data in a decrypted form. This discussion is well documented in international law enforcement forums with concerns raised under lawful access by the Federal Bureau of Investigation. In India, this turns into a bigger issue because investigative agencies get their authority to demand digital evidence through laws such as Section 91 and Section 92 of the Bharatiya Nagarik Suraksha Sanhita. On the contrary, these statutes become devoid of practical effect when a service provider is not able to hold any decryptable information. Inability to present clear-text evidence stalls the prosecutions, weakens objections in bail, and even forces the courts to withdraw charges for lack of corroboration. Thus the basic objective of criminal jurisprudence is frustrated, which is not only to protect rights but also to find the truth and do justice. With the rise in cybercrime and transnational threats, legal gaps fleshed out by E2EE are becoming a matter of considerable concern for Indian security infrastructure.[7]

---

[5] The Ongoing Debate Over Law Enforcement and Encryption, *available at:* https://onlinedegrees.kent.edu/blog/the-ongoing-debate-over-law-enforcement-and-encryption (Visited on February 18, 2025).

[6] National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers* 211 (The National Academies Press, Washington, DC, 1st edn., 2018).

[7] Robert E. Endeley, End-to-End Encryption, Backdoors, *and Privacy* 164 (ProQuest, U.S.A., 1st edn., 2020).

5. Legal Frameworks Governing Privacy and Digital Evidence

As the contention rages between protecting digital privacy and public safety, legal frameworks both at the domestic and international levels become reference points when rights, restrictions, and allowable intrusions are analyzed. These frameworks show permissible boundaries within which surveillance, interception, and the access to data are carried out, while simultaneously ensuring privacy, dignity, and due process in cases of illegal activities. During the Indian context, the legal apparatus must try its path through the constitutional guarantee of privacy and the legislative powers vested in state agencies for interception and investigation. Simultaneously, fulfilling international human rights obligations further makes the balancing act complicated. Legal frameworks are not cast in stone; they change through the acceptance and accommodations with technological changes, societal expectations, or institutional concerns. The advent of E2EE challenges the erstwhile investigative models and forces the legislature and judiciary to revisit the balancing exercise between civil liberties and collective security. In this line, the application of domestic laws, including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the procedural powers vested in agencies under the Bharatiya Nagarik Suraksha Sanhita, must be construed from an international human rights perspective so as to restore meaningful harmony between law enforcement and the right to privacy.[8]

6. International Human Rights Law

As the contention rages between protecting digital privacy and public safety, legal frameworks both at the domestic and international levels become reference points when rights, restrictions, and allowable intrusions are analyzed. These frameworks show permissible boundaries within which surveillance, interception, and the access to data are carried out, while simultaneously ensuring privacy, dignity, and due process in cases of illegal activities. During the Indian context, the legal apparatus must try its path through the constitutional guarantee of privacy and the legislative powers vested in state agencies for interception and investigation. Simultaneously, fulfilling international human rights obligations further makes the balancing act complicated. Legal frameworks are not cast in stone; they change through the acceptance and accommodations with technological changes, societal expectations, or institutional concerns. The advent of E2EE challenges the erstwhile investigative models and forces the legislature and judiciary to revisit the balancing exercise between civil liberties and collective security. In this line, the application of domestic laws, including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the procedural powers vested in agencies under the Bharatiya Nagarik Suraksha Sanhita, must be construed from an international human rights perspective so as to restore meaningful harmony between law enforcement and the right to privacy.[9]

1.1.5. Right to Privacy

The international legal regime imparts a rather strong normative framework that categorizes privacy as a fundamental human right. This global consensus tends to impact India's domestic jurisprudence and legislative drafting, whereby the courts often take recourse in international law to interpret constitutional provisions. International instruments of human rights safeguard the privacy of communication from unwarranted interference by the state. These instruments label national security as important but insist on the basis of the rule of law, wherein encroachment on the privacy interest must be: (a) lawfully carried out; (b) absolutely necessary in the interest of validity; and (c) proportionate. The principle of proportionality, which requires the examination of the right weighed against the restriction, becomes the foremost consideration in determining if laws that provide for access to encrypted data amount to violations of international human rights obligations. At the international level, deterrence efforts carry the obligation of countries to regulate surveillance in ways that defend individual autonomy and freedom from encroachment while simultaneously carrying out legitimate objectives such as crime deterrence and public safety. Being a signatory to vital international conventions, India is expected to interpret domestic statutes in consonance with the said commitments.[10]

1.1.6. Right to a Fair Trial under International Standards, Requiring Access to Evidence While Respecting Privacy Rights

While not binding in law, the Universal Declaration of Human Rights has immense normative weight and has been widely accepted as a source for identifying state obligations. Article 12 of the Universal Declaration states that no one shall now or at any time be arbitrarily or unlawfully interfered with respect to his privacy, family, home, or correspondence. This general defense, therefore, extends to all forms of communication, including those conducted by encrypted means. The same protection is further reinforced through Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which India is a party to as a legally binding treaty. The ICCPR prohibits unlawful or arbitrary interference with privacy, interception of family, or correspondence and requires the laws of the state to provide some degree of protection for these rights. These provisions require states to examine whether their intrusion into data access via policies, such as compelled decryption, backdoor access, or traceability requirements constitutes an 'arbitrary interference.'since in situations of E2EE, it is impossible, technically speaking, for a provider to access the content of messages, such demands raise important questions under international human rights law. The concern is not merely enforcing human rights but balancing the need for investigation with the right to engage in secure communication free from surveillance. Therefore, when discussing proposals that seek to weaken encryption or compel access to data, it is vital that India's regulatory framework be evaluated against international standards.

---

[8] O.L. van Daalen, "The Right to Encryption: Privacy as Preventing Unlawful Access", 49 *CLSR* 163 (2023).

[9] Greg Nojeim, Namrata Maheshwari, et.al., "Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth", 17 *IJLT* 94 (2021).

[10] Daniel Kardefelt-Winther, Emma Day, et.al., Encryption, *Privacy and Children's Right to Protection from Harm* 143 (UNICEF Office of Research - Innocenti, Florence, 1st edn., 2020).

Whilst international law strongly protects privacy, this protection is not absolute, especially when the right to a fair trial is involved. Article 14 of the ICCPR proclaims the right to "a fair and public hearing by a competent, independent and impartial tribunal." Such a right encapsulates procedural guarantees that permit the prosecution and defense to present evidence required for adjudication. The principle of fairness demands that States ensure the law enforcement agencies perform their work in gathering evidence through a procedure that respects privacy. The absence of a lawful access mechanism to E2EE communications may therefore affect the process of justice whenever these communications are relevant to establishing proof: evidence of guilt or innocence. This is particularly important in violent crimes, terrorism, or trafficking-related cases where encrypted data could be vital proof. On the contrary, international law absolutely forbids mass surveillance or the discarding of encryption for mere investigative convenience. Any mechanism for access to encrypted communication must be justified; it must be narrowly defined, and made available through transparent legal processes. For India, reconciling the competing demands of privacy and public safety entail judicial-legislative calibration to ensure that no apprehensions are raised against the enforcement of both "Article 14", as also "Article 17", of the ICCPR. Any other way would risk the very legality of the proceedings and also the digital credibility of privacy protection.[11]

7. United States

International human rights law provides privacy and fair trial protections and states put into place the working system for digital evidence to be accessed and the right to privacy to be enforced. The implantation of encryption technologies like E2EE creates major conflicts between an individual's legal rights and the state's need to investigate. In different jurisdictions, this balancing ends up being met with differing degrees of tolerance for encryption, according to their constitutional values, legislative traditions, and institutional structures. Domestic legislation and regulatory proposals within the United States and member states of the European Union dominate the global conversation on digital privacy, enforcement access, and limits of surveillance. These jurisdictions form the basis for the data-protection approaches with farther-reaching implications, including in India, where Indian courts and regulators often look at foreign law for guidance. The examination of legal architectures in these jurisdictions reveals the extent to which national frameworks can cope with competing imperatives. The approaches themselves critically pose many questions before Indian legal policymakers as they try to balance the protection of encrypted communications with the need for lawful investigative tools in an increasingly digitized society.

1.1.7. Fourth Amendment Protections Against Unreasonable Searches, Extended to Digital Data

For global privacy and surveillance issues, the U.S. has played the central role, with constitutional protections, federal statuary provisions, and legislative proposals placed as an example and a warning for democratic societies around the world. Digital privacy in American law is treated through two pans: that of constitutionally protected rights and legislative statutes. The U.S. Government recognizes the importance of encryption as being vital for protecting individual liberties and securing critical infrastructure but also is investigating potential regulatory regimes that do place restrictions on encryption under certain circumstances. The U.S. Department of Justice, the Federal Bureau of Investigation, and some other security agencies have repeatedly expressed concerns about the "Going Dark" phenomenon created by E2EE and its consequent effects on national security and criminal law enforcement. These issues have, in fact, given rise to policy proposals calling for technical workarounds, mandated content scanning, and even backdoor access, all of which create thorny constitutional and technical issues. The American framework demonstrates how difficult it is to legislate encryption in a manner that does not somehow undermine either security or the civil liberties it is meant to protect in the name of privacy and public safety.[12]

1.1.8. Stored Communications Act (18 U.S.C. § 2701 Et Seq.), Regulating Access to Electronic Communications

The Fourth Amendment to the Constitution bars unreasonable searches and also covers seizure by the state and has been interpreted by American courts to cover the various digital spaces, the phones, emails, and cloud storage. It is held by the courts that law enforcement is typically required to have a warrant from a judge upon probable cause before obtaining access to personal digital data. This requirement acts as a shield in the constitution to prevent any sort of invasive state surveillance. However, technological constraints prevent the reach of the Fourth Amendment in the case of E2EE. Law enforcement agencies cannot decrypt E2EE data even with a valid warrant because the keys reside only with the communicating parties. This lays bare an inherent incompatibility between constitutional guarantees and technological realities. The judiciary cannot compel service providers to provide content that they do not have in their possession. In this manner, Fourth Amendment jurisprudence is continuously evolving, with courts facing novel questions such as whether companies should be legally required to assist in decrypting or disabling encryption at the government's request. Interpretations that governments make in this regard ease far beyond the borders of the United States, as they become a precedent in the affair of how global digital companies set up their services and deal with government requests, including requests by jurisdictions such as India.[13]

---

[11] Encryption: Finding the Balance Between Privacy, Security and Lawful Data Access, *available at:* https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE (Visited on March 3, 2025).

[12] Ben Lutkevich, Madelyn Bacon, "End-to-End Encryption (E2EE)", *available at:* https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE (Visited on March 28, 2025).

[13] Encryption and the Digital Economy: Balancing Security, Privacy and National Security, *available at:* https://www.dsci.in/files/content/knowledge-centre/2023/Encryption-and-the-Digital-Economy.pdf (Visited on April 9, 2025).

1.1.9. Recent Legislative Proposals (Eff 2023 Review): Earn IT Act (S. 1207), Encouraging Content Scanning, Potentially Weakening E2ee; Stop Csam Act (S. 1199), Creating New Crimes That Could Impact Encrypted Platforms; Cooper Davis Act (S. 1080), Mandating Reporting of Drug-Related Activities, Raising Encryption Concerns

The Stored Communications Act (SCA), codified in "18 U.S.C., sec. 2701 et seq.", stands as a key element amongst the bigger umbrella legislation, the Electronic Communications Privacy Act (ECPA), and sets out how public authorities can compel service providers to disclose communications and records of customers. Under the SCA, agencies must follow different procedures according to the different kinds and ages of electronic data that they seek to obtain. Discrimination is made between content data and non-content metadata, with warrants, subpoenas, or court orders being required based on the sensitivity or intended use. But then came end-to-end encryption, which is effectively rendering most of the statutory schemes helpless. E2EE arose with the view that if a provider is compelled under the SCA to deliver content that is end-to-end encrypted, then it simply cannot comply. This is essentially a deadlock in the legal-technical tension, forcing investigators to shift strategies into accessing devices from suspects directly or utilizing advanced decryption avenues, which lie quite in ambiguous areas of ethics and law. These checkpoints amplify the call for a legislative refresh that accommodates modern-day encryption while maintaining an honor of privacy and due process rights.

8. European Union

An ongoing wave of legislative proposals has generated intense debates concerning the future of encryption. S. 1207, duly called the EARN IT Act, is promoted as a law to protect children and holds online platforms liable for user-generated content associated with child sexual abuse material. In order to encourage content moderation at the platform level, critics maintain that it might offer a backdoor incentive-for-e2ee to be weakened or shed entirely-going against the very spirit of E2EE. The other proposal, S. 1199, the STOP CSAM Act, might also increase the exposure to prosecution of E2EE platforms by introducing new federal offenses for online facilitation of child exploitation. The Cooper Davis Act (S. 1080) requires digital platforms to disclose suspicious drug-related activities, raising fresh worries about whether encryption can fit into the statute's reporting duties. These bills do not outlaw E2EE but create real legal pressures that may lead service providers to seek ways of either restructuring or disassembling encryption in a bid to lessen liability. The impact of such laws is felt worldwide. Indian regulators often refer to the American model in domestic debates on data protection and surveillance laws, thereby making it necessary to fathom how these American proposals may shape or provide justification for similar policy changes in India.[14]

1.1.10. General Data Protection Regulation (GDPR), Articles 5, 6, and 9, Emphasizing Data Protection and Lawful Processing (GDPR)

The European Union, compared to the United States, employs a more converse approach, focusing on fundamental rights and data protection issues. Under European law, privacy and data security are not considered mere legislative options but are instead mandated by charter- and treaty-based obligations. The GDPR and the ePrivacy Directive, forming the two pillars of data governance within the EU, set forth the legal standards pursuant to which personal data and electronic communications must be processed and protected. The EU further interlaces rules under the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union to maintain high levels of privacy, dignity, and freedom of expression. Within this ambit, E2EE is regarded as an essential technical standard to meet privacy obligations. Recognizing the legitimate needs of law enforcement for accessing data in the legitimate investigation and prosecution of crime, the EU, however, remains wary of any legal regime that would require encryption backdoors or weaken cryptographic protection. The European model, therefore, emphasizes privacy as a counterweight to enforcement-heavy frameworks and has influenced global discussions on encryption, including one in India.

1.1.11. Eprivacy Directive (Directive 2002/58/Ec), Safeguarding Electronic Communications Privacy

The General Data Protection Regulation is the most extensive and articulate data privacy law globally, and its principles are reflected in the "Articles 5, 6, and 9" of the Regulation. These articles maintain that personal data must be processed lawfully, fairly, and in a transparent manner, collected for specified legitimate purposes, and secured through appropriate technical and organizational means. Article 5 contains the core principles of data protection, which include data minimization, purpose limitation, integrity, and confidentiality. Article 6 provides circumstances in which personal data may be processed, such as the unambiguous consent of a data subject, processing necessary for the performance of a contract, performing a legal obligation, protecting vital interests of the data subject, carrying out tasks in the public interest or in exercise of official authority, or for legitimate interests pursued by the controller. By contrast, Article 9 handles the processing of sensitive personal data, prohibiting it in all cases other than those strictly laid down in the law. In this framework, E2EE is not only encouraged but sometimes even required as a basis for compliance under the data protection laws. Providers fulfilling the obligation of Article 5(1)(f) on appropriate security of personal data implement this by encrypting the user communication end-to-end. Weakening encryption for governmental or law enforcement access would put providers out of compliance and, therefore, could face heavy penalties under the GDPR. The penalties, or fines, under "Article 83" can be up to €20 million or 4% of the cost of global annual turnover, thus calling

[14] Decrypting the Encryption Debate: How to Ensure Public Safety with a Privacy-Preserving and Secure Internet?, *available at:* https://www.internetforum.eu/events/events/1127-decrypting-the-encryption-debate-how-to-ensure-public-safety-with-a-privacy-preserving-and-secure-internet.html (Visited on March 7, 2025).

for strong encryption by law and not as an option on policy grounds. These legal constructs substantiate the fact that GDPR goes a long way in indirectly promoting E2EE as best practices in data protection and hence puts more weight on the privacy side of the privacy-versus-public-safety argument.[15]

1.1.12. European Convention on Human Rights (ECHR) and Eu Charter of Fundamental Rights, Protecting Privacy and Expression (Sciencedirect Encryption)

The Directive on Privacy and Electronic Communications, or under its other name, the Privacy and Electronic Communications Directive (Directive 2002/58/EC), provides a specific framework for communications confidentiality that complements the GDPR. Public electronic communication service providers are bound by the directive to keep communications confidential and to neither intercept nor store communications without explicit permission of the user. Given this, from the standpoint of the Directive, it is clear that encryption technologies like E2EE are legally set for service providers so as to honor the users' confidentiality. The Directive provides that no interception or surveillance can be adopted by any party-public or private-unless the users clearly consent thereto or such interception or surveillance has been provided for as general exception by law. Any such exception must, however, be subjected to the tests of absolute necessity, proportionality, and legal precision. Attempts to enforce decryption or traceability mandates, such as those contained in India's "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", will find themselves under pressure scrutinized given the framework utilized by ePrivacy. Furthermore, as the European Commission progresses towards the adoption of ePrivacy Regulation, which would replace the Directive with a directly applicable regulation, legal protection for encrypted communications is likely to be strengthened even more. Such a legal ecosystem creates an environment where, on the one side, strong encryption is tolerated and is considered a bare minimum requirement for complying with regional data protection mandates. Where Indian lawmakers cast about for laying down their own privacy legislation statutes such as the "Digital Personal Data Protection Act, 2023", the EU model stands as an example to embed encryption within the legal mandate for data confidentiality.[16]

9. India

In addition to the aforementioned laws like the GDPR and the ePrivacy Directive, the pan-European legal frame is deeply rooted in the human rights instruments that protect personal privacy and freedom of speech. Article 8 of the European Convention on Human Rights (ECHR) guarantees respect for private and family life, home, and correspondence. A similar concept is advanced under Article 7 of the Charter of Fundamental Rights of the European Union, where respect for private communications is highlighted. These provisions have been interpreted by the European Court of Human Rights and the Court of Justice of the European Union to encompass digital communications and metadata. In this respect, encryption, which includes E2EE, is regarded as an essential way to facilitate the exercise of these fundamental rights. Any interference with encrypted communications through enforced backdoors or key disclosure mandates would thus have to meet the strict standards of legality, necessity, and proportionality under these human rights frameworks. The EU considers that weakening encryption amounts to undermining not just data security but democratic values with a chilling effect on freedom of expression; consequently, this will put at risk vulnerable groups such as journalists, activists, and whistle-blowers. The big consequences are that public safety, however important, cannot be the price to pay at the altar of fundamental rights. While not discounting the very real need for law enforcement to have access to digital evidence, the EU strives to seek solutions that do not compromise encryption or put personal freedom at risk. This draw-down norm so created continues to permeate through to reforms of data privacy even in countries as far apart from the EU as India, where courts have recognized privacy to be embedded under Article 21 of the Constitution of India, thereby giving insight into the legal and ethical boundaries involved in surveillance in the era of encryption.[17]

The Debate: Privacy vs Public Safety

Theme	Position	Key Arguments	Legal/Real-World References
Privacy Rights	Supports Strong Encryption	- Encryption ensures confidentiality and security in digital communication- Prevents unauthorized surveillance and data misuse- Safeguards personal liberty, democratic participation, and secure data flow	- Article 21, Constitution of India- Article 17, ICCPR- Section 69, IT Act, 2000- Section 20, Telecommunications Act, 2023
Freedom of Expression	Supports Strong Encryption	- Enables secure speech, association, especially for journalists, activists, and dissenters- Shields against retaliation, surveillance during protests- Prevents misuse of public order/national security laws to target dissent	- Article 19(1)(a), Constitution of India

[15] Anirudh Burman, "Considering India's Encryption Policy Dilemma", *available at:* https://carnegieindia.org/research/2023/11/considering-indias-encryption-policy-dilemma?lang=en (Visited on April 21, 2025).

[16] Pragya Jain, "Encryption: A Tradeoff Between User Privacy and National Security", *available at:* https://www.american.edu/sis/centers/security-technology/encryption.cfm (Visited on February 24, 2025).

[17] Equilibrium Between Security and Privacy: New Report on Encryption, *available at:* https://www.europol.europa.eu/media-press/newsroom/news/equilibrium-between-security-and-privacy-new-report-encryption (Visited on April 5, 2025).

Cybersecurity Concerns	Opposes Weakening Encryption	- Weakening E2EE introduces vulnerabilities exploitable by cybercriminals and hostile actors- Compromises systems used in banking, health, and governance- Reduces user trust in digital services and platforms	- Indian cases of cyberattacks on government and financial institutions
Law Enforcement Challenges	Favors Limited Access to Encrypted Data	- Encryption hampers criminal investigations into terrorism, child abuse, trafficking- Makes it difficult to gather usable digital evidence- Providers unable to comply due to technical constraints of E2EE	- Section 91, BNSS- Section 165, BNSS- Section 65B, Bharatiya Sakshya Adhiniyam
Real-Life Examples	Demonstrates Practical Challenges	- San Bernardino case: FBI unable to access terrorist's iPhone- Reflects global problem faced by Indian agencies too- Legal access does not equate to technical feasibility	- San Bernardino iPhone case (USA, 2015)- Section 100, Bharatiya Nyaya Sanhita
Digital Evidence Importance	Justifies Lawful Access	- Platforms like WhatsApp, Telegram used to share CSAM, plan terror attacks- Timely access can prevent harm and aid prosecution- Law enforcement seeks targeted, not mass access	- Europol 2024 report- Section 65B, Bharatiya Sakshya Adhiniyam
Balanced Legal Approach	Calls for Reform and Oversight	- Neither absolute privacy nor unchecked access is desirable- Requires strict judicial review, technical feasibility- Needs legislative reform and stakeholder cooperation	- Section 69, IT Act, 2000- BNSS investigation powers- Independent audits, proportionality tests
Ethical Considerations	Opposes Weakening Encryption	- Weakening encryption may lead to mass surveillance- Risks turning targeted surveillance into general monitoring- Reduces civil participation and trust in governance	- Information Technology Rules, 2009- History of surveillance misuse in India
Institutional Trust	Demands Accountability	- Trust issues with governments and corporations handling encryption keys- Lack of user consent, transparency, and oversight damages democratic norms- Ethical need for checks on surveillance power	- Lack of judicial pre-authorization for interception- Absence of enforceable remedies for unauthorized access

1.1.13. Case Studies and Judicial Precedents

India's approach to encryption and data access is essentially set within the framework of statutory laws, which have been created especially under the shadow of national security issues. Under "Section 69 of the Information Technology Act, 2000", both the Central Government and State Governments may intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource if sovereignty and integrity of India, defense, and public order stand on the way of such interest. Further, "Section 69A" empowers the government to block public access to information on similar grounds. The rules framed thereunder allow enforcement agencies to order intermediaries to decrypt. Anyway, in E2EE, even with such orders, service providers allege that they cannot decrypt a message because of the absence of access by them to user keys. This technical impediment has now rendered nearly all statutory instruments ineffective in the encrypted ecosystem. The recently enacted "Telecommunications Act, 2023", through "Section 20", further augments interception powers by allowing the suspension or interception of telecommunication services in the interest of national security or during public emergencies. Despite these provisions being enforceable by law, the absence of any judicial trappings and the veil of opacity they operate under raise constitutional questions, especially given the "right to privacy" affirmed under "Article 21 of the Constitution of India." Encryption poses a unique challenge here: on one hand, it benefits privacy and secure communication; on the other, it also frustrates the investigative and surveillance frameworks based on legal mandates that require extraction of readable information.[18]

10. Landmark Cases

The intersection between End-to-End Encryption (E2EE) and digital evidence access has dramatically became a legislative and technological challenge, and this has also seen courts in various jurisdictions being burdened with the matter of extreme contention. Courts have had to interpret constitutional protections in the evolution of technology, especially because the law enforcement agencies are facing greater and greater challenges in accessing

[18] Chamin Herath, Sneha Dawda, *Balancing End-to-End Encryption and Public Safety* 178 (Royal United Services Institute for Defence and Security Studies, London, 1st edn., 2022).

encrypted or cloud-stored data. Judicial precedents thus largely determine the treatment of encryption vis-a-vis privacy and public safety. These precedents also guide lawmakers and enforcement agencies in enacting, applying, or amending statutory provisions. In countries with written constitutions and strong rights frameworks such as the United States, courts have had to articulate how rights to privacy, due process, and protection against unreasonable searches come to be applied in the digital sphere. Though Indian courts have so far not made a ruling directly on E2EE, Indian jurisprudence often turns to comparative law in common law countries for assistance in interpreting "Article 21 of the Constitution of India." An examination of relevant precedents from jurisdictions such as the United States should help make more apparent the manner in which encryption and digital privacy can be reconciled with lawful evidence gathering, thereby providing useful insights to Indian courts and legislators as they confront comparable legal tensions.

1.1.14. United States V. Warshak (6th Cir. 2007): Established Fourth Amendment Protections for Email Privacy

The United States judiciary has taken on the role of coming up with the constitutional framework with respect to digital privacy. The decision in each case echoes an ever-increasing consideration by courts that the nature of privacy has changed for good in the digital era. Smartphones and cloud communication harboring an ocean of personal information-they may hold more information than an average home. Consequently, courts have held that legal protections need to be changed. Court decisions United States v. Warshak, Riley v. California, and Carpenter v. United States have set very powerful precedents, requiring that warrants be procured for access to digital content and thereby affirming that the powers of law enforcement must be constitutionally restrained. The aspects are different in these cases-electronic mailing, stored phone data, and location tracking-yet, combined, they establish that digital privacy deserves robust constitutional safeguards. The landmark rulings were based on the "Fourth Amendment to the United States Constitution", which guards against unreasonable searches and seizures; however, the substantive underpinnings and impetus behind judicial authorization would also find resonance in India, particularly as courts interpret "Section 69 of the Information Technology Act, 2000" regarding surveillance and "Article 21" on the right to privacy.[19]

1.1.15. Riley V. California (2014): Required Warrants for Cell Phone Searches, Affirming Digital Privacy

The Sixth Circuit Court of Appeals had to decide if a person has a reasonable expectation of privacy with respect to his stored email in United States v. Warshak. The Court said that the Fourth Amendment protects emails the same as it protects traditional communications, such as letters and telephone conversations. The Court thus established that government agents must procure a warrant supported by probable cause before compelling an email provider to disclose the contents of user communications. The ruling was important because it extended constitutional protections into the domain of cloud-based digital communication, which, before this ruling, was not well defined under the Stored Communications Act (SCA), which is the main statute regulating access to electronic records. The court reasoned that the users of such private messages have a reasonable expectation that the contents will be kept confidential, even if such messages are held or stored by a third-party provider. Hence, in the context of E2EE, the ruling is instructive-signifying that courts are prepared to require procedural safeguards prior to granting the government access to private communications. For Indian courts, where similar statutory power is found under "Section 91 of the Bharatiya Nagarik Suraksha Sanhita" and "Section 69 of the Information Technology Act, 2000", this Warshak dictum strengthens the view that digital data, encrypted or not, should be accessed only via judicial procedures that pay respect to users' privacy.[20]

1.1.16. Carpenter V. United States (2018): Mandated Warrants for Cell Site Location Data, Strengthening Privacy Rights

In the 2014 decision, the constitutional law judge of the United States Supreme Court determined with full consensus that investigators require a warrant to search any digital content in a suspect's cellphone, even when the person has been duly arrested. Using the wording of the opinion, the case involved a suspect arrested without a warrant for searching her or his smartphone, and that search yielded incriminating evidence. The court made a return to the distinction between physical objects and digital devices and held that cell phones containing vast amounts of sensitive personal data might not be treated like the rest of the items found on an arrestee. The court explicitly recognized that due to the nature of digital data—the volume, variety, and possible avenues to reveal almost everything about a person—such data should enjoy a higher degree of constitutional protection. In the domain of E2EE, the Riley case strengthens the position that encrypted data on a digital device should not be made accessible without proper judicial authorization. This case has implications for India, where law enforcement has the capacity to conduct searches under "Section 100 of the Bharatiya Nyaya Sanhita" but where the jurisprudential standards for searching devices are still an evolving debate. The Indian law does permit seizure of devices; however, the Riley case gives guidance that a warrant should be specific, proportionate, and have justification when it comes to digital content. This takes even more significance during the act of E2EE since decrypted data cannot simply be expected to be extracted without higher scrutiny.[21]

11. Conclusion

The ongoing debate on E2EE and digital evidence has underscored the changing challenges faced by the modern legal systems in trying to balance respectively fundamental rights and law enforcement imperatives. In India, where the right to privacy is now well under the umbrella of "Article 21 of

[19] International Statement - End-to-End Encryption and Public Safety, *available at:* https://www.homeaffairs.gov.au/nat-security/Pages/international-statement-end-to-end-encryption-and-public-safety.aspx (Visited on April 15, 2025).

[20] P. Hartel, R. van Wegberg, "Going Dark? Analysing the Impact of End-to-End Encryption on the Outcome of Dutch Criminal Court Cases", 12 *Crime Sci* 77 (2023).

[21] Understanding the Encryption Debate in India, *available at:* https://carnegieendowment.org/research/2021/09/understanding-the-encryption-debate-in-india?lang=en&center=middle-east (Visited on April 25, 2025).

the Constitution of India", any attempt to regulate or weaken encryption should thread with extreme care and constitutional sensitivity. Now indeed, encryption does prevent and hinder:certain types of digital evidence gathering in particular where these cases pertain to national security, child exploitation, or highly organized cybercrime but also acts as a firewall for millions of users requiring secure channels to communicate personally, in business channels, and politically. Investigative interests of the State remain legitimate and necessary; however, such interests cannot outweigh the Constitution without passing at least the tests of legality, necessity, and proportionality.

Right amid the eternal debate concerning End-to-End Encryption (E2EE) and access to digital evidence lie the ever-shifting challenges with which modern legal systems have to juggle fundamental rights along with law enforcement imperatives. In India, where for now, "Article 21 of the Constitution of India" is considered to guarantee a citizen's privacy, any attempt to regulate or weaken encryption needs utmost caution with respect to constitutional sensitivities. Encryption, conversely, also frustrates digital investigations, especially in certain cases dealing with national security, child exploitation, or organized cybercrimes; yet, encryption is likely to be the one and only barrier from the other side for millions of people who require secure channels of communication for their personal, professional, and political engagements. The interests of the state in investigation are both legitimate and necessary, but these cannot subliminally outweigh the constitutional mandate without standing the tests of legality, necessity, and proportionality.

According to the discussion so far, existing laws such as "Section 69 of the Information Technology Act, 2000", "Section 91 of the Bharatiya Nagarik Suraksha Sanhita", and "Section 100 of the Bharatiya Nyaya Sanhita" enable the state to compel disclosure and effect seizure by search. However, the provisions of these statutes do not account for an encryption regime wherein compliance is made impossible, not as an act of defiance but by intent. The inability for service providers to decrypt messages creates a completely novel category of legal deadlock-one wherein judicially authorized access orders contract with technological impossibility. This glaring disconnect necessitates a constitutional and technological recalibration of the law. The government must stay away from quick fixes like traceability laws or backdoors, which may appear expedient but that may harm the structural integrity of secure communication systems. Such approaches will adversely impact cybersecurity in India and Middle-East and beyond; international trust in Indian platforms; and Indian citizens'trust in the digital governance of their country.

Comparative analyses from jurisdictions such as the United States, United Kingdom, and Australia show that legislative attempts to subvert encryption often meet with public backlash, technical vulnerabilities, and judicial criticism. Technological solutions, such as client-side scanning, key escrow systems, homomorphic encryption, and secure multi-party computation, might be partial answers but come with legal and ethical ramifications of their own. The introduction of these in India would thus require a significant set of legislative amendments, as well as judicial clarifications and extensive discussion in the civil society. Equally important is that the implementation of alternatives occur in no legal vacuum. They ought to be grounded in the architecture of the "Digital Personal Data Protection Act, 2023", uphold the data protection principles contained therein, and include procedural safeguards corresponding to the ordinary procedural expectations under Indian criminal and constitutional law.