DIGITAL LOVE, LEGAL DILEMMA

Aastha Kumari, ICFAI University, Dehradun

Introduction

What happens when marital abuse becomes an excuse for surveillance and the court becomes the platform that validates it? Imagine your private chats, shared images, or late-night text being secretly downloaded without your consent and presented as an evidence, not by a hacker but by your own husband. Indian courts have begun to accept such evidence, arguing that a spouse's right to fair trial can override the other's Right to Privacy. This sets a dangerous precedent, especially in a country where one in three married women report domestic abuse, this judicial stance is blurring the line between justice and stalking. This article challenges that narrative, arguing that constitutional privacy can't be so easily surrendered at the altar of convenience.

Case Brief: The Madhya Pradesh Ruling

In a 2025 judgement, the Madhya Pradesh High Court allowed the use secretly obtained WhatsApp chats of the wife by the husband as an evidence where he accused his wife of adultery. The wife argued that the chats were obtained without her consent and it is violated her Rights to privacy under article 21 of the constitution. However, the court said that the right is not absolute and can be limited to ensure a fair trial. Further stating that the evidence in matrimonial dispute should not be excluded even if it gathered without consent according to the Family Courts Act. The court cited that in Puttaswamy judgement but gave more weight to husband's claim than to wife's right to privacy. The court, by overlooking how the evidence was obtained, raises concerns about weakening privacy protection in matrimonial cases.

Legal Framework: Can WhatsApp Chats Be Admitted?

According to Section 65B of the Indian Evidence Act, 1872 (mirrors in Section 61 of the Bhartiya Sakshya Adhiniyam, 2023), electronic record like chats and emails are admissible only if accompanied by a certificate authenticating the data source and method of extraction.

In Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Gorantyal (2020),

the supreme court said that electronic evidence without this certificate (in accordance with Sec. 65B Indian Evidence act) is inadmissible.

Still, the family courts often overlook procedural rigidity when it comes to digital proof of infidelity. This flexibility, while practical, comes close to crossing the line between practical decision making and staying true to the constitution. Courts must ask: is the method of gathering evidence necessary, legal, and the least harmful to the person's dignity?

Adultery After Joseph Shine: Civil Wrong or Moral Trail?

Adultery was a punishable offence under Section 497 of the IPC but after the judgement in Joseph shine v. Union of India, the Supreme Court struck down the section stating it as unconstitutional, upholding its several earlier decision. The court said that the adultery is matter of private affair and not a criminal. Additionally, the court also struck down Section 198(2) of the CrPC, which reflected complaints of adultery to be filed only husband, saying it to be violation of article 14 of constitution that states equality before law. This judgement decriminalized the adultery making it only a civil wrong for ground of divorce under Section 13(1)(i) of Hindu Marriage Act, 1955.

To prove adultery the parties, rely on circumstantial evidence such as – travel history, hotel stays, chat logs and digital messages. This trend invites both legal innovation and moral scrutiny. Can digital intimacy be used as a fact in courtroom without violating the right to privacy?

When surveillance become stalking

Surveillance inside marriage is often disguised as suspicion, concern, or moral authority. But when it includes unauthorized phone access, password threat and secret data extraction it becomes digital stalking. In India there are numerous Stalkerware application that allows users to download data without the consent or knowledge of the person being surveilled. News report indicate that the Ministry of Electronics and Information Technology (MeitY) is supporting the development of an act called "SafeNet" originally allowed parents to monitor their children's digital behaviour but now raises concerns about the potential misuse in intimate relationship. Are we legalizing stalking within marriage? The National Health Family Survey revealed that third of all married women aged 18 – 49 years have experienced spousal violence, making the

risk of digitally mediated abuse even more urgent to address. The feminist scholar and digital rights groups like Amnesty Tech warns that this is not just snooping it's a digital coercion, often rooted in broader patterns of marital abuse. If the judiciary doesn't establish a clear safeguard, it risks legitimizing coercive surveillance in the name of fair trial.

Suppose if a husband secretly accesses his wife phone to extract her intimate images she consensually shared with another person, and present them in court to prove adultery, this not only violates her dignity but also breaches Section 66E of The IT Act and her constitutional rights to privacy.

Right to Privacy & Constitutional Dilemma

The landmark judgement in K.S Puttaswamy v. Union of India (2014) said that privacy is not a peripheral privilege but it is a fundamental right under article 21. This includes our private message, personal photos, and digital life. However, in recent divorce cases the court allowed evidence like private chats or photos taken secretly from a spouse's phone without permission.

One such example is the recent judgement of Madhya Pradesh High Court, where the court said that maybe Right to Fair Trail is more important than the Right to privacy of an individual. "This shows a clear double standard – justice for one comes at a cost of another's fundamental rights." also raising a serious question. Can someone's privacy breached just to prove a point in the court?

The bigger problem is this : should a system allows this kind of surveillance just because it helps someone win the case?

In a country where privacy is a fundamental right, the courts need to ask: are we protecting justice, or encouraging people to break the law on the name of justice?

Comparative jurisprudence: Lessons from Abroad

As legal systems worldwide confront the complexities of privacy in the digital age, matrimonial disputes have emerged as a particularly sensitive area. The way different jurisdictions handle private digital evidence—such as phone records, messages, or location data—offers crucial insight into how a balance between personal dignity and judicial truth-seeking can be achieved.

In the United Kingdom, the protection of personal data is enshrined in the Data Protection Act, 2018, which works in harmony with the General Data Protection Regulation (GDPR). This legal framework mandates that any collection or use of personal data, including information on a spouse's device, must be lawful and based on consent. Courts in the UK have taken a consistent stance that even within marriage, one individual cannot intrude into another's private communications without legal authority. Unauthorized access to digital devices, even in the context of divorce proceedings, can result in civil penalties or criminal liability—an approach that reinforces the principle that privacy does not dissolve within domestic relationships.

In the United States, privacy protections derive primarily from the Fourth Amendment, which prohibits unreasonable searches and seizures by the state. A key doctrine that has shaped American evidence law is the "fruit of the poisonous tree" principle, first articulated in Silverthorne Lumber Co. v. United States (1920) and later clarified in Nardone v. United States (1939). This doctrine excludes from court proceedings any evidence that is derived from illegal or unconstitutional conduct. In Mapp v. Ohio (1961), the U.S. Supreme Court extended this exclusionary rule to the states, reinforcing that evidence obtained through violations of constitutional rights cannot be used in court.

However, U.S. states differ in how strictly they apply these protections. In New York, the courts have maintained a rigid approach, as seen in People v. Weaver (2009), where the state's highest court held that warrantless GPS tracking of an individual's vehicle was unconstitutional. The judgment reinforced the idea that even basic location data enjoys privacy protection. On the other hand, California has interpreted the right to privacy more flexibly. In People v. Diaz (2011), the court ruled that police could search the contents of a suspect's mobile phone without a warrant during a lawful arrest, suggesting a more relaxed view of privacy when a device is shared or accessible in public spaces.

These international models demonstrate a careful legal balancing act. They acknowledge the value of evidence in judicial proceedings, but they also recognize that how that evidence is obtained matters. The integrity of the legal system depends not only on uncovering the truth, but also on upholding individual rights in the process.

By comparison, Indian law is still catching up. Although the Supreme Court, in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), declared the right to privacy a fundamental right under Article 21 of the Constitution, its implementation in family law and evidence law remains

inconsistent. While Section 65B of the Indian Evidence Act, 1872, outlines procedures for presenting electronic records in court, it does not address whether evidence obtained through a breach of privacy—such as hacking a spouse's phone—should be excluded. This silence often leaves courts to make subjective judgments, leading to uncertainty in how digital privacy is treated during matrimonial disputes.

India stands at a crucial point. As technology becomes more entwined with human relationships, there is a growing need to codify the limits of digital intrusion in civil proceedings. Drawing on established practices from the UK and the US could help Indian courts craft a more structured, rights-respecting approach to digital evidence—one that reflects the values of a modern constitutional democracy.

The way forward: Balancing the trust and Technology

As digital communication becomes an inseparable part of modern relationships, the Indian legal system must evolve to ensure that technological advancement does not erode foundational values such as trust, dignity, and due process. In matrimonial litigation, where emotions often run high and privacy boundaries become blurred, courts must proactively lay down clear procedural and ethical guidelines regarding the admissibility and collection of private digital content.

It is imperative that courts discourage the emerging trend of spouses assuming the role of digital vigilantes—secretly accessing mobile phones, email accounts, or cloud storage in pursuit of evidence. Matrimonial disputes should not devolve into private surveillance warfare. The family court's mandate is not criminal investigation but dispute resolution with compassion, grounded in mutual respect and fairness. The judicial process must guard against any normalization of unauthorized surveillance within domestic spaces, no matter how emotionally charged the context may be.

To strike a balance, digital evidence should only be admitted when it is obtained legally, voluntarily, and in strict compliance with the procedural safeguards outlined under Section 65B of the Indian Evidence Act, 1872, read with relevant provisions of the Information Technology Act, 2000. Section 65B specifically mandates that electronic records must be accompanied by a certificate authenticating their source, integrity, and method of production. This requirement serves as a safeguard against manipulation and infringement of privacy, particularly in cases

where devices are accessed without consent.

Furthermore, judicial training and public legal awareness campaigns are essential. Courts must educate litigants on the crucial distinction between legitimate suspicion and unlawful intrusion. While evidence of adultery, cruelty, or financial misconduct may be relevant to a matrimonial proceeding, it must be sourced in a manner that does not violate constitutional rights—especially the right to privacy under Article 21, as affirmed by the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017).

Additionally, courts should consider implementing in-camera proceedings or confidential digital evidence protocols, where sensitive materials are examined in a restricted setting, ensuring that personal dignity is not further compromised in the name of legal inquiry. Psychological harm resulting from exposure of private content—such as personal photographs, chat logs, or voice notes—must be acknowledged and mitigated through thoughtful procedural design.

As the proposed Digital Personal Data Protection Act, 2023, moves towards implementation, there is an opportunity for family courts and policymakers to jointly develop data ethics frameworks within civil litigation. This would not only clarify admissibility standards but also create a rights-based ecosystem where truth does not come at the cost of human dignity.

Ultimately, the way forward lies in recalibrating legal standards to reflect the dual realities of trust and technology. Courts must walk a fine line—preserving evidentiary integrity while upholding the individual's right to autonomy and privacy, even in the most adversarial of personal disputes. It is only through this careful balancing act that justice in the digital age can remain both effective and humane.

Conclusion

The increasing use of private digital content in matrimonial cases presents a serious legal and moral dilemma. However, the main aim of court is to serve justice but this should not come at a cost of violating fundamental rights. The Madhya Pradesh High Court’s acceptance of secretly obtained evidence may seem like a procedural efficiency, but it sets a dangerous precedent where illegally gathered, privacy-violating data is normalized in the court.

If the judiciary continues to allow such evidence without examining how it was obtained, it risks encouraging surveillance within marriage, especially by the more dominant spouse. This not only contradicts constitutional privacy under Article 21, but also opens the door for digital abuse, coercion, and revenge porn.

For balancing the right to a fair trial with the right to privacy, the courts must set clear limits. Justice can't be built on personal violation. Surveillance should not become the new normal thing in matrimonial cases; dignity must remain at the centre of due process.

REFERENCES:

1. *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* [2017] 10 SCC 1 (SC).

2. *Joseph Shine v Union of India* [2018] SCC OnLine SC 1676.

3. *Anvar PV v PK Basheer and Ors* (2014) 10 SCC 473.

4. *Arjun Panditrao Khotkar v Kailash Kushanrao Gora.ntyal and Ors* (2020) 7 SCC 1

5. 'Wife's WhatsApp Chats Can Be Valid Evidence in Divorce Proceedings: MP High Court' The Economic Times (22 March 2024) https://economictimes.indiatimes.com/news/india/wifes-whatsapp-chats-can-be-valid-evidence-in-divorce-proceedings-mp-high-court/articleshow/108665987.cms

6. Information Technology Act 2000, Section 65B, Section 66E.

7. Indian Evidence Act 1872, Section 65B.

8. Data Protection Act 2018 (UK) https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

9. Regulation (EU) 2016/679 (General Data Protection Regulation).

10. *Silverthorne Lumber Co v United States* 251 US 385 (1920).

11. *Nardone v United States* 308 US 338 (1939).

12. *Mapp v Ohio* 367 US 643 (1961).

13. *People v Weaver* 12 NY3d 433 (2009).

14. *People v Diaz* 51 Cal 4th 84 (2011).

15. Amnesty International, 'Snooping Isn't Just Snooping': Tech-Facilitated Gender-Based Violence in India (Amnesty Tech, 23 November 2022) https://www.amnesty.org/en/latest/research/2022/11/india-tech-facilitated-gender-based-violence/

16. Centre for Internet and Society, India's Parental Control Directive and the Need to Improve Stalkerware Detection https://cis-india.org/internet-governance/blog/india2019s-parental-control-directive-and-the-need-to-improve-stalkerware-detection

17. International Institute for Population Sciences and Ministry of Health and Family Welfare (India), National Family Health Survey – 5 (2019–21) https://nfhsiips.in/nfhs5.php