

Why the law is yet to crack the digital privacy code

Himanshi Dhawan : 8-10 minutes

You may believe that a road rage investigation involving a collision and verbal altercation can hardly spiral into an inquisition. Journalist Abhishek Upadhyay discovered it the hard way that the long arm of the law can stretch backwards in time into a person's digital world — a gated and private enclave of an individual — to mine information far beyond what's required. When Upadhyay was faced with an FIR in August and what he considered to be intrusive prying into his personal life and work, he rushed to the [Supreme Court](#). The Ghaziabad police had sought access to his phone records from June 1 onwards to investigate a road rage incident that allegedly took place on Aug 18 this year. He told the court that the police had also sought data from social media intermediaries, including YouTube and X, covering a period well before the date of the alleged offence. This included Upadhyay's international mobile equipment identity (IMEI) number, which uniquely identifies a mobile device. Interestingly, it was Upadhyay who had flagged the misappropriation of donations at the Ayodhya temple and alleged that he was being framed for that. SC then questioned the police, asking it to explain why the information was needed, putting a pause to what appeared to be a search for unearthing his sources as Upadhyay alleged. It stayed his arrest, too. The tussle between evidence gathering by investigative agencies and an individual's [right to privacy](#) and against

self-incrimination

is, however, only intensifying. The implementation of Bharatiya Sakshya Adhiniyam (BSA) and Bharatiya Nagarik Suraksha Sanhita (BNSS) in July 2024 set the stage for the conflict. Wide-ranging powers Legal experts say the law doesn't have enough safeguards to protect individuals. Anuj Berry, lawyer and partner at law firm Trilegal, says the laws were designed for physical "filing cabinets", not devices holding a lifetime of data. Under the Indian Evidence Act, enacted in 1872, a search-and-seizure operation by the police meant a physical search of the suspect's house by checking cupboards and safes, and looking under the bed. The boundaries were clear, visible and tangible. "When BNSS expanded these powers to include electronic communication, it added no corresponding safeguards. The law conflates seizure (taking the device) with search (examining its contents). Once seized, no separate authorisation is needed to image (mirror) the device," Berry says. And unlike a safe that may have a limited number of contents, our phones are now a portal to our lives. Cyber law expert Prashant Mali explains the scale of the problem. "A phone is no longer merely an object, it is almost a digital autobiography of its owner, with chats, photographs, financial and health information, location history, professional communication and, sometimes, confidential journalistic or legal sources. Therefore, seizing a handset and examining everything inside it cannot automatically mean the same thing," he says. Berry points out another serious anomaly. "There is a regulatory asymmetry where real-time interception requires strict

judicial oversight

but accessing stored data on a seized phone requires none. The constitutional limit on compelling the revealing of passwords or providing biometrics also remains unsettled due to conflicting court decisions.”Lawyers describe this as a “fishing and roving expedition” where an individual is arrested and his or her digital device seized and cloned even before the judicial process kicks in.Experts point out that in the Upadhyay case, access to phone records was demanded without any independent authorisation or showing a requirement for information related to the June-to-August window.“The court happened to intervene here because it was politically sensitive and was brought to its attention. In many cases, such matters may not come to the court’s attention at all,” says an academic.Without that scrutiny, the same absence of oversight can play out far more brazenly. In October 2021, the Hyderabad police stopped commuters on a busy street to check their phones for chats about drugs. It was only after a severe backlash that the police said it was part of a crackdown but hastily withdrew the anti-drug drive.

As seen in Upadhyay’s case, legal experts say agencies are often hoping to recover evidence which is a clear violation of the right against self-incrimination. Several court orders have allowed police to access biometric details from the accused to unlock a phone while ruling that an accused cannot be forced to reveal his or her password.Cyber law expert Mridul Bhatt, writing in Indian Journal of Law and Legal Research, says, “However, this distinction collapses in practice because unlocking a phone by any method gives the police access to deeply testimonial content, making the act of unlocking functionally equivalent to compelled self-incrimination.”In February, two Jamia students had approached Delhi High Court, asking for their biometric data (collected by Delhi Police when they were questioned for merely participating in a campus protest in April 2025) to be deleted.They also demanded that Criminal Procedure (Identification) Act, 2022 — used to collect biometric details — be declared unconstitutional and void for “disproportionately infringing on the right to privacy, right against self-incrimination, as well as the guarantee against arbitrary state action” which remains pending before the court.What the law lacksExperts agree that any state action to access personal digital data must meet the 2017 privacy judgment’s three-part test — legality, necessity and proportionality. It broadly means that there must be a law in place; the invasion of privacy must be for a legitimate state aim, like solving a crime; and there must be a rational link between the aim and invasion.The state should not use a sledgehammer to crack a nut. The warrant or authorisation should effectively say what are you looking for, why do you believe it is there, what period of data is relevant, and what offence does it relate to.“It should not be like ‘Give me your phone and I will first read your entire life and then decide what may be relevant,’” says Mali.A petition by the Foundation for Media Professionals seeking a digital doctrine has been pending since 2022, following which a committee was set up by the Union government in 2023 but the issue has remained pending. Former SC judge Justice Madan Lokur says, “Experience of the past few years is an indication that a law must be enacted with necessary constitutional safeguards.”Zealous investigative agencies, often pressed for time and resources when trying to catch criminals, may be tempted to bypass laws. They could, in fact, do worse.Earlier this month, grainy CCTV footage revealed what appeared to be two police personnel allegedly placing a phone in the house of Noida-based labour activist Srishti Gupta. The activist had been arrested and her phone seized

in April. Yet, the visuals appeared to show the police placing Srishti's phone in her house to be "seized" later. Releasing the footage, Gupta's lawyer accused the police of "planting evidence". The police have denied the allegation but the jury is out on what may have happened. Former Pune police commissioner Meeran Chadha Borwankar says that time is of the essence in investigations but officers do need to be trained in legal processes. "Clear rules help but a transparent and well-documented/video-recorded recovery of any instrument used for a crime shall withstand judicial scrutiny. Our IOs need to be trained in legal processes involved in recovery extensively and regularly," she says. Berry explains how the legal process can help in this regard. "A reasoned court order must be obtained to examine a device's contents, distinct from the order to seize it. In urgent cases, access must be regularised by a warrant within a fixed period (e.g., 48 hours), failing which the material becomes inadmissible. The orders must specify the offence, categories of data, date ranges and search terms. The examination must be confined to these defined terms."