

Can police make you unlock your phone? It depends on how it's locked

By: **Anuj Berry** (Partner), and **Aryan Agrawal** (Associate)

The Kerala High Court has held that just because a suspect has information about a crime in his phone, the police can't seize it without following established legal procedure.

The Kerala High Court [held](#) on 10 July that the police can't seize a suspect's phone without following the procedure established by law. The suspect, a journalist, had approached the court with a grievance that the police seized their phone without implicating them in any crime or being called as a witness in an investigation. The court held that "simply because the journalist has got some information about the crime, the mobile phone cannot be seized..."

While the law regarding phone confiscation is in place in India—that is, a warrant is required—whether an officer can, after seizing a phone, compel a suspect to unlock their phone and access the data in it has the unfortunate lawyerly response of 'it depends'. The law is muddled on this issue.

Muddled law on phone privacy

The Karnataka High Court has previously [held](#) that a suspect has no right to refuse to divulge their passcode or not provide their biometrics to an officer seeking to unlock their mobile devices for an investigation. The case was filed by a Bengaluru techie who was suspected of offences under the narcotics Act and refused to disclose the password of his mobile phone and e-mail addresses to the police officers. The officers filed an application seeking an order to direct the suspect to disclose the password. The high court ruled that a suspect has no fundamental right to refuse to divulge the password to an officer, saying recognition of such a right would result in a chaotic situation where investigating officers would be unable to perform their duties.

In contrast, the Special CBI court in New Delhi has [held](#) that a suspect cannot be compelled to divulge the password of their mobile devices either by an officer or by a court as it would impinge upon the fundamental right to privacy and the right against self-incrimination guaranteed under the Indian Constitution. The right to privacy is an inviolable constitutional right, which inter alia sets certain limits on the extent of state surveillance and intrusion into an individual's private life. Right against self-incrimination, recognised under Article 20(3) of the Indian Constitution, provides that "no person accused of any offence shall be compelled to be a witness against himself".

In a similar vein, the Code of Criminal Procedure (CrPC) states that a suspect is not bound to answer those questions that "would have a tendency to expose them to a criminal charge or to a penalty or forfeiture". Under these constitutional and due process safeguards, individuals can choose to remain silent and not be compelled to provide 'personal testimony', which may incriminate them in criminal proceedings. The right against self-incrimination kicks in when information based on the 'personal knowledge of the suspect' is sought and when it is required to 'furnish a link in the chain of evidence'. Thus, compelling a suspect to provide passcode details can be a violation of their fundamental right if it is perceived as self-incrimination.

The CBI court had said in its judgment that when a suspect is asked to disclose their password, they are required to recall it through personal knowledge, which would fall within the category of a testimonial fact. Further, the entire purpose of this testimonial fact would be to utilise the data in the mobile device to establish further links in the chain of evidence. Therefore, a direction compelling a suspect to disclose their password would amount to self-incrimination and be hit by Article 20(3) of the Constitution.

Interestingly, based on this sequitur, the CBI court drew a difference between the protection afforded under the law for passwords/pattern-drawn security features and biometrics (finger impressions, face or iris recognition) to unlock phones. An accused can be directed to give their biometrics to unlock mobile devices. Unlike passcodes, biometrics are only physical evidence that do not require attribution of personal knowledge when used. Thus, according to the CBI court order, an officer can direct you to unlock your phone using your biometrics but not by asking you to type out the password or by drawing the security pattern to unlock your phone. In other words, using your mental faculty to remember your password to unlock your phone is akin to testifying against yourself, but using biometrics is not.

Indian law and technology

This peculiar situation depicts the failure of law in India to evolve with technology, exacerbated by the age-old tussle between law enforcement's duty to investigate crimes and the individual's fundamental right to privacy and the right against self-incrimination. This balancing act that leaves both sides treading on thin ice ought not to be further muddled by unnecessary semantics and splitting of thin hair. Surely, the technological method of locking your phone should not determine whether an officer can collect evidence against you. As it happens, the CBI court declared the judgment of the Karnataka High Court "with due respect and high regard... to be not correct" and *per incuriam* i.e., passed without regard to the laws laid down by the Supreme Court. Interestingly, the CBI court stands at a lower footing and hierarchy than the Karnataka High Court, making it unusual to pass any comments on that decision. The act of the CBI court proceeding on its own notion and contradicting with the Karnataka High Court's decision could itself be called *per incuriam*.

The law is far from settled in India on such matters. The Apple-FBI encryption dispute in the US and the [recent](#) EnconChat dispute in the EU indicate other jurisdictions are also struggling to answer this query. A writ petition on this issue was filed by a group of journalists [last year](#) before the Supreme Court of India. The matter is notified to be tentatively listed at the end of this month. While the answers to these questions get settled in courts, one would perhaps do better to contact their lawyer and get appropriate counsel when confronted with such unlocking requests.

Anuj Berry is a Partner and part of the Disputes practice at Trilegal, India's top-ranked full-service law firm. Aryan Agrawal is an Associate at Trilegal. Views are personal.

This article was originally published in The Print [here](#).