THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

December 3, 2022

On Digital Devices and Criminal Investigations

By: Abhinav Sekhri

We need judicial courage in reclaiming the silences in our laws, which were designed for a time when privacy did not matter, to protect the rights of citizens during search and seizure of digital devices such as phones and computers.

Preamble

It has been 20 years since mobile phones and other personal digital devices stopped being simply 'computers'. Thanks to the internet, they have become a part of life itself for many persons. The flipside of this reliance upon handheld devices and the like is that there is no need to go very far to find out where a person keeps her most intimate secrets: everything is there, behind a fingerprint, face scan, or not-so-random password. It is no surprise that these personal digital devices have slowly come to occupy a central position in investigations into alleged crimes. Whether it is the taxman, or police, or the Enforcement Directorate or the Central Bureau of Investigation, everyone wants to look at the phone, believing that it would be key to solving the case.

What are the legal issues in search and seizure of personal digital devices?

A Digression

For a long time, international law was dominated by something that is called the 'Lotus Principle'. Named after a famous judgment arising from the collision in the Mediterranean of the French steamer SS Lotus with the Turkish steamer SS Bozkourt in 1926 that came before the Permanent Court of International Justice, the principle essentially stood for the idea that nation states were free to do anything so long as there was no express prohibition against that course of action. Or, to put it more bluntly, everything not expressly illegal, is legal. It may be immoral, controversial, contrary to norms and principles, but it may also not be illegal.

Why recount the Lotus Principle from international law while discussing mobile phones and police investigations in India? This is because, surprisingly, this principle offers a handy summary of how the law interacts with enforcement agencies searching and seizing personal digital devices in India.

In an era where digital devices are often an extension of the self, they become obvious targets for agencies hungry for information about their suspects. The suspects, in turn, have good reason to contest agencies rummaging through their personal life to any degree more than strictly necessary. In such a scenario, the tussle between state interests and citizens can only be mediated by the law. But what happens where the law is silent on many of these aspects that require its mediating influence? The state then turns back to the Lotus Principle to claim that all that is not expressly prohibited — asking the suspect to unlock a device, copy all its contents, make multiple copies, etc. — is permitted.

> The conduct of agencies in demanding access to devices and making copies is not some vengeful design of an individual officer, but a product of how the legal framework is. There is no respect for privacy because the framework was designed for a time when privacy was an irrelevant consideration.

Both the state and citizen can contest that the law is not silent but in fact supports their respective positions. That has largely been the playbook so far in litigation and is something that I will explore here too. It is equally important to contest the silences, which I would argue will ultimately prove more critical not only for the more specific issue of the privacy of information contained in personal digital devices but recalibrating the balance between state interests and citizen rights in the sphere of criminal investigations.

The Murky Legal Waters

Powers of search and seizure, along with the power to question persons, are one of the most widely recognised powers of law enforcement agencies towards gathering evidence for the prosecution of crime. The nature of this evidence has witnessed dramatic changes over time, especially with the advent of the digital revolution. The search and seizure provisions though, have not seen any real change from their first iteration in the criminal codes of the mid 19th century, and have formed the bedrock for investigations under other special penal statutes that have come up over time.

Sections 91 to 102 of the Criminal Procedure Code of 1973 bear a direct lineage to the erstwhile criminal procedure codes of 1861, 1872, 1882 and 1898. This means that the statutory provisions in force today continue to be those that were designed at a time when citizens were subjects devoid of basic autonomy and dignity, and a criminal procedure code was little more than a tool to rationalize the expression of the sovereign's ultimate power to prosecute and punish.

Given this set of assumptions, it is natural that the legal framework deals with issues with a broad strokes approach with little space for nuance. It focuses on ensuring maximum discretion for the police (or courts) to authorize taking anything that may bear even remote relevance to an ongoing inquiry or investigation. There is no prerequisite to obtain warrants for conducting search, giving police broad leeway to proceed in the face of emergent circumstances. The warrant regime itself carries barely anything by way of checks and balances — so much so that general warrants permitting searches of places without any need to satisfy of the kind that were frowned upon in England at the time were permitted.

> A privacy respecting regime houses a search and seizure law that is designed to disregard any notion of privacy.

It is no wonder, then, that applying this search and seizure regime would enable outcomes that give any notions of privacy a complete go-by. The conduct of agencies in demanding access to devices and making copies is not some vengeful design of an individual officer, but a product of how the legal framework is. There is no respect for privacy because the framework was designed for a time when privacy was an irrelevant consideration.

Privacy is no longer an irrelevant consideration, of course. The search and seizure regime came to be questioned on the anvil of the Constitution early in the life of the Republic, in a case where it was argued that the search and seizure violated a right to privacy that was now secured to citizens. By a detailed decision in M.P. Sharma v. Satish Chandra, the challenge was rebuffed by the Supreme Court in 1954 when it cited the absence of a specific clause securing a right to privacy to Indian citizens. Puttaswamy swept aside this view in 2017 and affirmed that the Constitution of India also secures a right to privacy to all persons.

The result is a contradiction — a privacy respecting regime houses a search and seizure law that is designed to disregard any notion of privacy. To resolve this contradiction, it is being argued that the terms of the search and seizure laws ought to be read in a manner consistent with the right to privacy. Or it is being argued that the existing search and seizure regime is entirely inapplicable to the digital realm, premised as it is on physical spaces. We are then left with a deafening silence in the law which needs to be filled.

Reclaiming the Silences

One would argue that Puttaswamy and the recognition of the right to privacy would put the matter to bed by requiring a reconsideration of the validity of the search and seizure regime. Such a view would give too little credit to the complexity of the decision, which, while affirming the existence of privacy as a right in the abstract, left its specific determinations in each context to the future. If anything, whatever little authority has emerged so far has also treated the absence of illegality as suggestive of legality behind such actions.

The Karnataka High Court in Virendra Khanna rationalized the absence of narrow tailoring in the search and seizure regime to safeguard individual privacy by concluding that this was not a place where privacy reigns supreme. A detailed opinion ultimately held that constitutional recognition of a fundamental right to privacy only meant that now it was imperative to comply with the privacy-denuding procedure of law and did not find any problems in the procedure itself. It seems then that we have come a long way from where we started this article; from needing the Lotus Principle to citing express permissions in the form of judicial opinion to support police seizing devices without warrants, forcing them open, and making copies wholesale.

> What is needed is a resounding demolition of ideas such as the Lotus Principle that are premised on a logic of an unbridled sovereign power without any regard for the citizen.

The issue has now reached the Supreme Court where the impetus will be to place the contradiction at the heart of the matter in sharp relief. Asking for stricter application of an existing regime which is inconsiderate of privacy cannot somehow magically safeguard that right. Efforts must be to try and soften the edges of the colonial regime to meaningfully secure the right to privacy. Reading in a warrant requirement to install judicial scrutiny, limiting access to only what is relevant, having a process for requesting deletion of copies — all of these are small steps to reclaim a modicum of dignity for the citizen entangled in the process.

For this interpretive exercise to be successful, it is much more important for judicial courage in reclaiming the silences in our laws rather than myopically focus on the finer details. What is needed is a resounding demolition of ideas such as the Lotus Principle that are premised on a logic of an unbridled sovereign power without any regard for the citizen. Such a theory can have no place in a democratic republic with a system of laws founded upon limited government, where citizens are recognized for possessing inviolable dignity and autonomy.

> Rather than the individual clawing away at state power and having the burden to show its illegitimacy, it is the state that must satisfy courts on its reasons for clawing away at the zone of personal liberty and autonomy.

How would such a judicial approach look? It would, for starters, begin by dismantling any notion of presuming that the actions of government (not Parliament) are legitimate, and replace this with a presumption of the inviolability of individual dignity. Rather than the individual clawing away at state power and having the burden to show its illegitimacy, it is the state that must satisfy courts on its reasons for clawing away at the zone of personal liberty and autonomy. Focusing only upon search and seizure in the context of digital devices without bringing in such a change would be akin to missing the forest for the trees.

Conclusions

The Lotus Principle reflected unbridled sovereignty on the international stage and the tendency for reducing international law to little more than an apologia for state power. It was not a creation of the Permanent Court in 1926 but an affirmation of the legal approach that had developed over millennia on the assumption of sovereign power being absolute. Laws and rules were but a means to rationalize the expressions of this power and could not constrain it, especially in arenas such as discipline and punishment (See The Police Power: Patriarchy and the Foundations of American Government by Markus Dubber (2005) for a fuller exposition of this though). Constitutionalism, liberal democracy, and limited government, have all been part of the relatively nascent recent attempts to invert this founding assumption and in fact constrain the leviathan by demanding a justification for its power and not merely serving to rationalize it.

Simply introducing a constitution and representative government are hardly enough to replace the schools of thought that have guided us for millennia. It takes more effort than that, which is what India has also witnessed. Despite the Constitution of India recognizing various fundamental rights and safeguarding individual dignity, it has not yet managed to dismantle that assumption of state power being absolute in some contexts. Courts continue to uphold the power of the sovereign to adopt whatever means necessary to secure discipline, despite a written instruction to disavow that very assumption. It does not help that the state was content in retaining statutes that were designed for a time when the laws did not ask questions of the sovereign, placing an even greater burden on the courts to continuously reimagine square pegs to slot them into round holes.

> Despite the Constitution of India recognizing various fundamental rights and safeguarding individual dignity, it has not yet managed to dismantle that assumption of state power being absolute in some contexts.

This conflict is in essence what presents itself where personal digital devices are being sought for purposes of criminal investigations. There is an obvious implication of privacy, but the conflict is determined by laws for whom privacy was an alien concept, throwing the burden upon our courts to resolve the matter. Of course, privacy is not the only consideration involved. Where the state machinery comes down against persons accused of crimes to try and coerce them into giving up passwords, that implicates an additional set of rights most notably that against compelled self-incrimination which were alien at the time when the law was conceived. The same exercise ensues: the state enforces the archaic law that does not consider the target of investigations as invested with rights. This citizen enforces her constitutional claim, requiring courts to balance the interests of the state in pursuing investigations while ensuring that the constitutional right is not left a dead letter.

By and large, courts have refrained from embracing their role of the watchmen in this sphere of criminal law and procedure by adopting a highly deferential attitude to state power and contorting themselves into unseemly shapes to somehow justify the vesting of wide discretion in the face of individual dignity. Thus, in this context of mobile phones, giving passwords is seen by courts as not giving ‘evidence’, and the only way to secure privacy is to insist upon strict compliance with an obstinately privacy-denuding regime. Thus, forcing me to give the key to my apartment, and then ransacking it to find one piece of paper, ends up being justified in the process.

There have been dissonant notes, of course, giving us a glimpse of what a legal regime that insists on holding the state accountable for violating individual dignity looks like. It was at heart of the proportionality doctrine that was considered favourably by the Supreme Court in the Puttaswamy decisions. It is this vision of the relationship between the state and citizen which must inform how courts turn to the problem of law enforcement agencies demanding access to mobile phones and other personal digital devices.

[Disclaimer: the author is part of the legal team assisting the Petitioner in W.P. (Crl.) No. 395 of 2022 before the Supreme Court of India where these issues are at stake]

Abhinav Sekhri is a lawyer practising in New Delhi. When not working or writing about criminal law, he can be found trawling through the archives in search of curious stories from Indian legal history.