The good and the bad of the privacy ruling

One of the pleasures of being a lawyer in a vibrant common law jurisdiction is that every once in a while the system spits out a decision so artfully crafted and filled with nuance and meaning that it is a sheer joy to read. Few decisions in recent memory are better exemplars of this than the recent decision of the Supreme Court in Puttuswamy v. Union of India, affirming the fundamental right to privacy.

The system of common law is based on precedent. Judges are bound to consider past judgments and apply them to disputes that come before them in the future. They are only permitted to diverge the chain of historical decisions if it is possible to sufficiently distinguish—in fact or principle—from the available precedents. Our law is, therefore, not so much a monolith handed to us by our founding fathers as an edifice constructed brick-by-brick through an incremental series of decisions—each one based on the judgements that preceded it but in aggregate a composite, well-integrated whole. Common law takes shape in this manner, organically evolving to accommodate new technologies and social mores while remaining consistent with the past from which it arose.

The fundamental right to privacy has been developed by the courts in this manner for over 60 years. The reason the Supreme Court had to take the effort to gather nine judges together to rule on whether or not we have a fundamental right to privacy was because of a minor inconsistency that had crept into the chain of decisions over 50 years ago and remained, till last Friday, unresolved.

It all began when the attorney general of India, while defending the Aadhaar project, argued that the Constitution does not include within it a fundamental right to privacy. He based his conclusion on two cases decided by the Supreme Court—one, MP Sharma v. Satish Chandra, decided by an eight-judge bench in 1954 and the other, Kharak Singh v. State of Uttar Pradesh, by six judges in 1962. Both cases had held, under different circumstances, that the Constitution of India does not specifically protect the right to privacy. In the 55 years that have passed since these cases were decided, there hasn't been a larger bench of Supreme Court that has considered this issue, and therefore, by sheer weight of numbers, these judgements bound us. It would take nine judges to set this straight.

When you get into the weeds, MP Sharma dealt with a completely unrelated issue—the right against self-incrimination. While it did mention the right to privacy in passing, these comments were stray observations at best. Kharak Singh, on the other hand, was a confusing decision that held, on the one hand, that the intrusion into a person's home is a violation of liberty (relying on a US judgement on the right to privacy), but on the other hand went on to say that there was no right to privacy contained in our Constitution.

But since these were eight- and six-judge benches of the Supreme Court, every subsequent court had to deal with this confusion as best they could. In the next case, Gobind v. State of Madhya Pradesh, a three-judge bench, mindful of its inability to overturn a judgment of a larger bench, skirted around the inconsistency by "assuming" that the right to privacy was protected under the Constitution—relying on the first part of the Kharak Singh judgement without specifically calling out its inconsistency with the second. Once Gobind hacked a pathway through this thicket, many smaller benches followed suit, building on these principles to articulate a fundamental right to privacy in the context of medical privacy, matrimonial privacy, reputational privacy, privacy of sexual orientation and many more. But we always knew that this jurisprudence, built as it had been on uncertain foundations, was susceptible to challenge.

The task before the nine-judge bench in Puttuswamy v. Union of India was to settle the law once and for all. They did so emphatically—overruling both MP Singh and Kharak Singh to the extent that they had held that there was no fundamental right to privacy. They also overruled additional district magistrate (ADM) Jabalpur—a decision that allowed for fundamental rights to be suspended during an Emergency and called into question the judicial reasoning in the Naz Foundation case that implied that the “minuscule minority” LGBTQ (lesbian, gay, bisexual, transgender and queer) community was not entitled to the right to privacy. They connected our privacy jurisprudence over the years with our international commitments and established our conformity with comparative laws around the world.

In doing so, they affirmed the precedential basis of every single privacy judgement in our judicial history, making it clear that even without an express fundamental right to privacy, we are entitled to enjoy the right as it is inherent in our right to liberty and dignity.

Much as I enjoyed reading the judgement, I have some misgivings about the direction down which it is pointing us. I am concerned that the tests they have articulated and the constraints they have imposed could well have a chilling effect on our ability to get the most out of modern technology. While the opinions of both justice D.Y. Chandrachud and justice Sanjay Kishan Kaul speak of the need to balance the individual’s right to privacy with the benefits of data mining and big data, they go on to suggest a framework to protect individual autonomy based solely on consent. While they seem to understand the benefits that big data can bring us, they appear, at the same time, ignorant of the chilling effect that a strict notice and consent-based framework can have on these business models.

Just as the strength of the common law system comes from the solid foundations on which it is based, its weakness is that it is structurally designed to build only on past decisions. Since they are required to decide solely based on historical thought processes, they are incapable of finding solutions for a future untethered to the past. This is why a common law judiciary is so bad at dealing with disruption.

We are currently in the midst of a period of unprecedented disruptive change. Where it was once sufficient to secure personal privacy by limiting the collection of data, in the face of a rapidly increasing number of devices and systems that constantly collect information from us in ways that we cannot completely comprehend, consented collection is completely infeasible. We are also beneficiaries of new technologies that leverage the power of data offering us facilities and services that enhance our quality of life. Most of these new technologies rely on big data and machine learning—which in turn depend on access to large data sets in order to do their magic. Requiring data controllers to restrict themselves by proportionality and purpose could have a chilling effect on these new business models.

Regulators around the world have begun to discard the principle of notice and consent that guided their actions for over three decades. They have, instead, begun to rely on models such as accountability to address the challenges of a disruptive future. If the nine judges who have done such an exemplary job of righting the mistakes of the past could have only shifted perspective while legislating for the future, we’d have got a judgement that was truly perfect by every measure.

Rahul Matthan is a partner at Trilegal. Ex Machina is a column on technology, law and everything in between.

His Twitter handle is @matthan

END