O.P. Jindal Global University
A Private University Promoting Public Service

Law & Policy BRIEF

Jindal Global Law School
India's First Global Law School

Horizontal Application of the Right to Privacy: A Much Needed Measure

Vol. IV | Issue 5 | May 2018

The recent right to privacy judgment by the Supreme Court has rightly imposed on the state a duty to respect the right to be let alone. Now the judiciary must take the next step and recognize that the fundamental right to privacy extends to private entities as well. This is especially so because of the rise of colossal online entities which scoop up enormous amounts of personal data and impose severe costs on users in the process.

INTRODUCTION

The right to privacy has not always been embraced by the Indian judiciary. Indeed, uncertainty reigned over whether such a right existed for many years, with the judiciary going back and forth on the issue. So when the Puttaswamy judgment hailed the right to privacy as a fundamental right many celebrated it as a transformative decision that settled the distinctive place of privacy in our constitutional order.

It may be disappointing therefore to be faced with the prospect that Puttaswamy did not fully address some key questions pertaining to the right to privacy. In all the decades of deliberation during which the place of privacy has been questioned by judges the engine of technological innovation has completely transformed the world in which we live. As a result the perspective of privacy that has undergirded judicial discourse is in urgent need of an upgrade.

For instance, much of the conventional discourse around right to privacy applies the concept to state. This is based on the understanding that the government represents the most significant threat to our right to be let alone. Certainly this is a legitimate concern. States routinely abuse their surveillance powers at the expense of the citizenry, especially in the wake of 9/11 when the ruse of national security has been deployed as an all-purpose justification for infringing cherished liberties.

It is also undeniable that governments unrestrained by a watchful judiciary can quash citizen rights with impunity. It cannot be gainsaid therefore that Puttaswamy strikes a major blow in favor of individual rights when it circumscribes the ability of the state to intervene in the lives of citizens.

Many scholars have heaped praise on the decision for the novel way in which it valorizes the concerns of the individual. This is a refreshing and much needed articulation of the safeguards provided by the constitution against a state that has regrettably been overbearing on more than a few occasions.

In our collective focus on the government, however, we have perhaps allowed the burgeoning private sector to slip by unnoticed. Judges and lawmakers need to be acutely conscious of the changed landscape of private business activity that occurs online, especially given that private sector invasion of privacy often serves as a conduit for governmental violation of privacy.

I] THE RISE OF PRIVATE SECTOR SURVEILLANCE

The recently arrived at consensus in Puttaswamy about the centrality of privacy to our scheme of fundamental rights seems at first glance to be inapplicable to the burgeoning regime of online private sector companies that proffer a business model of free use of their platforms in exchange for the ability to mine the data generated by users. After all, private companies monitor citizen activity to enable advertisers to market their wares to those most likely to purchase them. There is an element of mutuality wherein consumers also benefit by gaining greater access to goods and services.

On the face of it, this is a far cry from the incentives driving government monitoring of citizen activity. While monitoring of our shopping habits is designed to help us as per the business model of private companies it is no one's contention that widespread government monitoring of ordinary citizen activity such as the metadata generated by online political activities is contributing to public welfare.

About the Author

Sachin Dhawan *is Assistant Professor and Assistant Director, Centre for Law and Humanities, Jindal Global Law School [JGLS]. He teaches constitutional law and family law. His scholarly work has focused on the intersection of religion and law in India. He has written for numerous outlets on subjects ranging from electoral politics to the Uniform Civil Code. Professor Dhawan was closely involved in the conception and formation of the Jindal School of Liberal Arts and Humanities, established in 2014.*

At best governments can claim the right to engage in targeted surveillance of nefarious foreign entities and individuals and their local associates who wish to do harm.

However this seeming disparity between harmless private and harmful public invasion of privacy breaks down upon further examination. Consequently, the protean nature of internet commercial activity requires a far more robust engagement by the judiciary on the question of how far the right to informational privacy extends.

II] ABUSE OF PRIVACY BY THE PRIVATE SECTOR: THE HIGH COST OF "FREE" SERVICES

Supporters of private sector surveillance counter that consumers cannot legitimately claim a right to privacy given that most internet platforms are free. Such claims made in defense of internet companies offering their services for free are misrepresentative. They obscure the manifold ways in which these companies are in fact imposing a cost on their users. Given the ubiquity of the danger posed, it is imperative that courts unambiguously recognize and apply the horizontal right to privacy even against those entities and platforms that offer their services for free.

Online companies may not be charging their users directly, but they are eviscerating their privacy. In making this case, the judiciary should highlight the fact that online sites run by private behemoths can manipulate user conduct. Recent exposes have conclusively established that there are ways to influence the behavior of users unbeknownst to them.

For instance in 2014 it was revealed that Facebook surreptitiously used almost 700,000 members as guinea pigs in an experiment to establish whether "emotional contagion" could be achieved by sprinkling users' news feeds with disproportionately positive or negative words. Emotional contagion, which refers to the widespread manipulation of mood states, is not a legitimate use of privately collected data, especially when the data is generated by Indians and the contagion is spread at the behest of a foreign entity. It does not do anyone any good to pretend that mood manipulation is not qualitatively different from tracking users to help them shop better.

Furthermore, "research has also shown that voting behavior can be influenced by undetectable social networking maneuvering."The United States is currently embroiled in a political controversy arising out of the possible manipulation of Facebook data in order to assist the 2016 presidential campaign of Donald J Trump. However as Time magazine detailed in a prescient article several years ago, Facebook was used in the 2012 presidential campaign to favor the re-election campaign of then incumbent Barack Obama.

Despite the surface appearance of neutrality projected by Facebook, therefore, "there is a thumb on the scale that users are lulled into ignoring and Facebook is complicit in this confusion…as they often present themselves as a trusted information conduit..."

Recent disclosures also bring to light the way in which Google played a role in the 2012 U.S. Presidential election. Author Julia Angwan details the ostensibly neutral search engine's involvement in her book 'Dragnet Nation.' As she puts it, "[s]earchers who looked up Barack Obama saw news about the president threaded into their future searches on other topics. Searchers who looked up Mitt Romney did not see news about the Republican presidential candidate included in subsequent searches."

India has also experienced some controversy surrounding the use of private individual data by political parties for partisan purposes. Cambridge Analytica, a U.K. based firm has allegedly deployed data generated on social media platforms to help manipulate people into voting one way or another at the behest of certain political parties.

As indicated earlier, user data could be sold to unscrupulous entities such as those on the "dark web." Recent news reports have been peppered with disclosures of large scale data breaches and hacks.

The U.S. company Equifax is but one of a host of entities that has recently succumbed to this seemingly omnipresent brand of cybercrime. The data cache siphoned off as a result of such hacks "is often bought and sold…by identity thieves looking to make money off your good name—and any numbers or information associated with you."

We also have to consider the fact that when data is stored anywhere in large quantities it is very prone to abuse "by stalkers and rogue employees." As Angwin points out, the instances of abuse of data by those with access occurs all too frequently. She substantiates this claim by providing examples of people whose data trails have even gotten them killed. In one example a mentally disturbed man commissioned an "online data broker" to find the address and other personal details of a woman he was obsessed with - tragically he killed her and then himself upon obtaining this information.

In addition data breaches are costly. Given the ever expanding reach of the online ecosystem it is no surprise that many more commercial transactions are now conducted online. From hotel reservations to grocery shopping we tend to prefer the convenience of digital transactions. However the volume of sensitive financial information that is stored with various private entities as a result exposes us to significant financial harm.

III] THE MYTH OF CONSENT

While the harms described above inflict rising costs and adversely affect the lives of many unsuspecting consumers, there has emerged in public discourse a litany of responses from the champions of private sector exceptionalism. One of the propositions almost universally invoked by defenders of internet companies is that people who join their free platforms do so consensually.

However given the extensive uses to which individual data is put, consent is a chimera. People cannot possibly be aware of the thousands of ways in which the data they generate is being deployed, examined, traded and stored.

Indeed it has been said that "[c]onsent in fact is rendered almost irrelevant – it is almost impossible to obtain consent from an individual when data that is collected can be used for multiple purposes by multiple bodies." Online activity is not about a series of discrete transactions wherein one can agree or disagree about whether and how their data will be exploited. Rather "at any given time, unless a user's browser is protected by a robust anti-tracking extension, the personal computer is making between 50-100 connections – if not more, and without consent or prior knowledge – to other websites that track, store and share data." For each person to continually give consent for potentially thousands of uses if not more is an impossible task.

Thus whatever consent is being given by clicking the appropriate button below a 'terms of service' pop up on an internet platform does not include many uses to which data is put by the platform itself or the entities that the platform sells to.

A corollary of the myth of consent peddled by internet companies is that those who do not use their platforms do not get tracked. This is a patently false assertion. Mark Zuckerberg has clearly stated in recent testimony before the U.S. Congress that Facebook collects data even on those who don't have an account. This is made possible "…through the use of cookies place[d] on their machines…" when they access "publicly available Facebook content" or visit a site that uses technology belonging to Facebook. Whatsapp also has access to data of those who are not a part of Whatsapp. The tracking engendered by cookies makes consent irrelevant. Even if one only visits a website but does not sign up to become a member one's data is subject to exploitation. Making matters worse is the fact that Facebook does not permit non users to find out what the company knows about them.

IV] HORIZONTAL RIGHT TO PRIVACY AND THE STATE ACTION DOCTRINE

It can be seen from the above discussion that 'free' online services impose a significant cost on users and that the notion of consent is meaningless. However, if courts are to step in to remedy the tremendous damage being done as a result to users' privacy, they must discard certain shibboleths about the propriety of intervening in the affairs of private enterprises.

Traditionally courts in India do not apply fundamental rights to private entities. This is because of article 12 of the Indian constitution, which calls for the application of fundamental rights to 'state.' However, courts have in some circumstances held the state responsible for private sector violations of fundamental rights, either because the state did not enforce existing law protecting individual fundamental rights or because the state did not institute a law protecting individual fundamental rights. In Puttaswamy for instance, the Supreme Court has called on the government to protect and uphold the right to privacy by instituting a robust data protection law.

There is another way around the conundrum of the state action requirement, to protect the privacy rights of Indians irrespective of whether a data protection law is enacted. While application of the fundamental right to privacy via a writ petition filed under article 32 against a private entity may not be feasible, it is possible to take action under article 226 of the constitution. This article empowers High Courts to "issue to any person or authority, including in appropriate cases any government suitable orders to enforce fundamental rights."

In this way, article 226 provides that the respondent may be a private entity. The Supreme Court has endorsed this argument in a series of cases. In the Zee Telefilms case, the Supreme Court asserted that while private entities may not be challenged under article 32, that does not exempt them from the application of fundamental rights via article 226. This position was further entrenched by the Court in the Cricket Association of Bihar case, wherein it confirmed that private bodies performing public functions can be made subject to the fundamental rights via article 226.

It is argued here that social media giants and other large conglomerates with a deeply pervasive online presence perform a vital public function. They function as gatekeepers to online speech, which is increasingly becoming a preferred mode of communication. More people are now in touch through Facebook and Whatapp than ever before, expressing thoughts and exchanging ideas. Companies which facilitate such extensive communication are in a position to harm the interests of their customers, as detailed above. Just as states have to be curbed from abusing their extensive powers through the application of fundamental rights, it is fast becoming evident that companies which constitute the online marketplace of ideas have to be held to account for their users' privacy. As per the logic of the extension of fundamental rights to private sector companies, whenever an entity exercises disproportionate power over individuals, an obligation is created to check its ability to abuse the citizenry.

CONCLUSION

Indeed Puttaswamy represents a promising beginning in the uphill climb to recognize the rights of individuals vis-à-vis private companies. Albeit in the context of the state, the judgment clearly places the individual at the heart of its analysis of the right to privacy. This is something that the General Data Protection Regulation [GDPR] an EU law that came into effect on May 25 2018 also emphasizes.

Perhaps future judicial engagements with the right to privacy can build on the model and the philosophy embodied in the GDPR.

This should be done especially with respect to the concept of informed consent. As indicated earlier, while it may be possible for a user to assent to a vaguely worded set of terms and conditions that fails to limit what internet companies can do with data, such consent is hardly meaningful. At the same time, it would be practically impossible to grant genuine consent for the actual uses to which data is put by the numerous entities of the internet ecosystem.

Consequently unless the judiciary draws a firm line in the sand with regard to the explicit need to obtain user consent, our data will remain hostage to the whims and fancies of private sector mercenaries. Facebook is almost certainly not alone in refusing to divulge the full extent to which it tracks its own users. We are probably not even fully aware of the proliferation of technologies now in existence to facilitate user tracking. The impunity with which individual data is seized upon and deployed to generate profit is fast resulting in the complete evisceration of privacy. Moreover, companies will not stop at collection of data. Dystopian visions of chips being embedded in employees to track their movements have already been mooted and are perhaps not so far off from implementation. Already there have been instances in the United States of software being used to track the activities of school students. Courts must prevent such Orwellian nightmares from turning into reality.

End Notes

1. Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors
2. The Snowden disclosures brought to light the close, even symbiotic relationship between the U.S. government and private companies. The government secured access to citizen data generated online by, in large part, compelling private conglomerates to hand over data being collected by them without the complete knowledge of users.
3. Robert Scheer, They Know Everything About You Pg. 39
4. http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters/
5. Robert Scheer, They Know Everything About You Pg. 39
6. Julia Angwin, Dragnet Nation: A quest for privacy, security, and freedom in a world of relentless surveillance, Chapter 1
7. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
8. Julia Angwin, Dragnet Nation: A quest for privacy, security, and freedom in a world of relentless surveillance, Chapter 1
9. https://thewire.in/economy/internet-big-data-inequality-digital
10. https://thewire.in/economy/internet-big-data-inequality-digital
11. http://www.bbc.com/news/business-36854292
12. http://www.bbc.com/news/technology-36671941
13. Zee Telefilms v. Union of India (2005) 4 SCC 649
14. Board of Control for Cricket in India v. Cricket Association of Bihar 2015 (3) SCC 251

About the O.P. Jindal Global University

O.P. Jindal Global University (JGU) is a non-profit global university established by the Government of Haryana and recognised by the University Grants Commission (UGC). JGU was established as a philanthropic initiative of its Founding Chancellor, Mr. Naveen Jindal in memory of his father, Mr. O.P. Jindal. JGU has been awarded the highest grade 'A' by the National Accreditation & Assessment Council (NAAC). JGU is one of the few universities in Asia that maintains a 1:13 faculty-student ratio and appoints faculty members from India and different parts of the world with outstanding academic qualifications and experience.

JGU is a research intensive university, which is deeply committed to its core institutional values of interdisciplinarity and innovative pedagogy; pluralism and rigorous scholarship; and globalism and international engagement. JGU has established eight schools: Jindal Global Law School (JGLS), Jindal Global Business School (JGBS), Jindal School of International Affairs (JSIA), Jindal School of Government and Public Policy (JSGP), Jindal School of Liberal Arts & Humanities (JSLH), Jindal School of Journalism & Communication (JSJC), Jindal School of Art & Architecture (JSAA) and Jindal School of Banking & Finance (JSBF).

Editors and Conveners of the Law and Policy Research Group

Dr. Ashish Bharadwaj is an Associate Professor in Jindal Global Law School, and a founding editor of the Law & Policy Brief. He serves as Director of Jindal Initiative on Research in IP & Competition (JIRICO) at O.P. Jindal Global University, a visiting professor at Institute of Innovation Research in Tokyo, and an affiliated faculty of CIPR, Maurer School of Law in Indiana University Bloomington. He holds a B.A. (Hons.) and M.Sc. in economics from Delhi University and Madras School of Economics, LL.M. in law and economics from Rotterdam, Hamburg and Manchester, and Ph.D. from the Max Planck Institute for Innovation & Competition in Munich.

Sannoy Das is an Assistant Professor at Jindal Global Law School. He holds a B.Sc. LL.B. (Hons.) from National Law University, Jodhpur and read his masters[1] in law from Harvard Law School. He researches on questions of law and history, international trade, political economy and political theory. Prior to joining the academy, he practiced law at the High Court at Calcutta. At the law school, apart from teaching courses on civil litigation, international trade and interdisciplinary electives, he also co-ordinates moot court activities.