21 MARCH 2016 | BUSINESS | CYBERLAW

What Did The Apple Say To The Skeleton Key?

Two players from the tech space on whether an individual's privacy can be compromised in the name of national security

NIKHIL PAHWA, KARNIKA SETH

No battle around technology in recent times has captured the public attention as much as Apple vs FBI in the US. The American government and the FBI have been pushing Apple to open up the security code of the iPhone belonging to one of the San Bernardino killers. Apple has been resisting, citing privacy and information security issues. Google and Facebook have come out in support of Apple. The question is whether an individual's privacy can be compromised in the name of national security or even a police investigation. To find out how such a debate would play out in India, Outlook invited two players in the tech space to weigh in:

"Those Who Own Our Data Own Us"

We are data. In bits and bytes, we are the websites we surf, the comments we leave, the texts we send, the social networks we log on to, the videos we forward, the bills we pay, the subsidies we receive, the advertisements we click on. As more people and devices connect to the internet, it is inevitable that more of what we do will get digitised, collected and stored: what we eat, when we leave home, which flights we prefer, what time we go for a run or hit the gym. Some of this data we give voluntarily—for subsidies and benefits, or even to health apps, for monitoring and assessing our performance. Some of it we give without realising: for example, details of where we are when we update Facebook, whose profile we check on the sly. Some of it we would never want anyone to get access to, which might make us vulnerable: the illnesses we carry, the people we flirt with, the things we bitch about, what we message our lawyer and our doctor about.

The argument I hear most frequently about privacy is that if you have nothing to hide, you have nothing to fear. This is far too simplistic an approach, because the lack of privacy impacts vulnerable communities the most: it could be a friend from the LGBT community who wants to discuss about coming out, or someone who's facing sexual harassment at the workplace, and wants to discuss with you about whether they should go to courts or not. It's not whether we have something to hide or not, but whether someone can trust us with information that they want kept private.

"This is where the FBI's efforts hurt most: by forcing Apple to create a backdoor entry into a system Apple itself can't peek into, the FBI is making everyone vulnerable."
Nikhil Pahwa, founder MediaNama

data can own us. For democracy, at the core of which are individual rights and civil liberties, it is essential that our data belongs to us, and we have the choice to recall it, and not give up control over it.

This is where the impact of what the FBI is trying with Apple hurts most: by forcing the company to establish a backdoor entry into a system which even Apple can't peek into, it makes everyone vulnerable. Governments across the world are pushing for lower encryption norms because that will help them break into all digital communications and storage, and check whether someone is a terrorist or not.

India's draft encryption policy, which was put on the backburner last year, expected citizens to store all their communications in plain text for 90 days and banned bulk encryption systems. Such attempts create a system which not just the government but also hackers can exploit to compromise our security. Once such systems are built into software and communication networks, you will be vulnerable; the easier it is for governments to access your data, the easier it becomes for hackers as well.

There are legitimate national security concerns as well: to protect citizens, governments need to be able to access communications quickly, and identify potential terrorist threats. The United States has its National Security Agency (NSA), and India is setting up its Centralised Monitoring System, to spy on citizens. This breaks one of the fundamental, foundational principles of our democracy. We need to work towards systems that ensure user privacy, and treat requests related to national security as exceptions and not the norm. Access to private information, in each instance, must be under strict judicial oversight, instead of allowing the state the opportunity to put in systems that let them access everything about us.

Nikhil Pahwa

"Public Interest Over Privacy"

Apple's legal tussle with the FBI has opened a Pandora's box. Should privacy be protected to the extent that it overrides needs of law enforcement? Should cooperation be extended by technology companies to law enforcement agencies in cybercrime or terrorist attack cases? Should law and public safety or national security be compromised in the name of protecting individual privacy? Should commercial considerations and security concerns surpass law enforcement needs or effective dispensation of justice?

Unless technology firms cooperate with law enforcement agencies and investigative bodies, effective investigation of such crime cases will not be possible. Law, in that case, will remain merely a paper tiger. Electronic evidence is by far the most important evidence in many offline/cybercrime cases; and it is crucial in tracing criminals misusing technology to commit illegal acts that aim to harm a nation.

Considering India is yet to sign a cybercrime convention, efficient cooperation from technology companies whose servers are based abroad is indispensable for enforcement of laws. Such cooperation is expected from all technology companies, including Google, Facebook, WhatsApp and others, whose high-security encryption services may be misused. A similar debate arose in India regarding Blackberry, where law enforcement agencies required the messaging service to disclose certain data and monitor communications or shut down its services. However, fishing expeditions are strongly declined and only in case of reasonable suspicion and prima facie evidence can law agencies request for such data.

In India, the right to privacy is protected by Article 21 of the Constitution. However, this right is not absolute, but remains "subject to procedure established by law". Section 69 of the Information Technology Act, 2000, empowers the government to issue directions for interception or decryption of any information through any computer resource. However, this power is to be exercised only when it is satisfied that it is necessary in the interests of sovereignty or integrity of India, the defence of India, friendly relations with foreign states, maintenance of public order, and so on.

Section 69(3) puts an obligation on a subscriber or intermediary or any person in charge of the computer resource to extend all facilities and technical assistance to provide access or secure access to the computer resource. By virtue of Section 69(4), the intermediary, or subscriber, or a person who fails to assist the investigation agency, is punishable with imprisonment for a term that may extend to seven years and shall also be liable to pay a fine. Section 69B

"Unless technology companies cooperate with law

to three years is prescribed. Similarly, there's Rule 3 (7) of the IT (Intermediaries Guidelines) Rules, 2011, that mandates an intermediary to provide all assistance to government agencies in such matters.

Clearly, if this Apple versus FBI battle were to be fought in India, the law of the land would prevail. A person's privacy is certainly not greater than protecting the interests of one's nation or the public interest. Technology companies argue that developing such software for decryption of passcodes will lead to weakening of their security, but surely they cannot blindfold themselves and allow terrorists to misuse its security features too! We did not give up inventing smartphones for fear of its misuse by some. In the same vein, we cannot give up inventing decryption software to protect law of the land, its nation and its people!

Karnika Seth

agencies, effective investigation of national security cases will not be possible. Law, in that case, will merely remain a paper tiger."
Karnika Seth, cyberlaw expert, adivsor to govt agencies

READ MORE IN:

NIKHIL PAHWA | KARNIKA SETH | BUSINESS

NEXT STORY : BIZTRO

MORE FROM OUTLOOK INDIA

To Make India A Global Leader, BJP Should Win All Polls From Panchayat To Parliament For 50 Years: Amit Shah

BJP Leader Arrested For Sexually Assaulting Minor Girl In Train

Would The BJP Nudge The RSS To Appoint A Dalit Or Adivasi As Sarsanghachalak?

YOU MIGHT ALSO LIKE