BW BUSINESSWORLD

That Thing We Called Privacy

The new Aadhaar Act will make unprecedented intrusions into your privacy. But Internet companies already know more about you than the government ever will

Nine years ago, back when Facebook was still this strange online thing you 'poked' friends on, when Google was still trying to hard-sell Gmail, and when Edward Snowden was just a young computer wizard with the CIA; the American Civil Liberties Union put out a video of what ordering pizza would be like in the future.

The video, on Youtube, shows how, with access to just the credit card records of the caller, one can have ready access to the customer's address, medical records, data on recent travel plans (including discounted tickets), waist size based on a recent purchase, and whether the credit card limit has been maxed out. All those intimate details, to improve the pizza buying experience.

Thankfully, today, ordering a pizza in India is still not quite so creepy or intrusive an experience. But, it's no secret that there are companies that possibly know more about you than your mother does and are busy making money with the data — with your permission, of course.

Identity Known

And now, the government wants in on this as well. In March, the Aadhaar Act, 2016 (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) was passed creating a legal framework built around the unique number that will double up as an identifier for the Indian citizen — a one-stop solution for placing you. Should that scare you?

Section 7 of the Act says the government may mandate the identity of a citizen be pin-pointed before he is eligible to

receive any subsidy, benefit or service that involve any money spent out of, or received into, the Consolidated Fund of India. And as we all know, between LPG, ATF and electricity subsidies, there was hardly anybody in the country who is not a beneficiary of a government dole. The Prime Minister recently pushed for land records to be digitised and synced with Aadhaar. Over time, the identification could become de facto mandatory for all transactions, without being ostracised and penalised. Suddenly, information that was so far scattered across the banking channel becomes consolidated for easy access.

A surreptitious leak (though prohibited by the Act), or an order from a district judge is enough for the government to profile just about anybody in the country.

Elonnai Hickock, director – Internet Governance, at CIS, Bangalore, summarises it best: “With the Aadhaar Act, it seems the government took the concerns that were voiced about the UID scheme and rather than addressing them, used the legislation to give legal backing to the issues that were of concern.” The reference is to the ongoing Supreme Court case on whether the Aadhaar ecosystem violated the right to privacy, where the Attorney General famously claimed that we don’t even have a right to privacy in India.

But why is that such a bad thing? The American Civil Liberties Union website has documents relating to the ongoing case in the US about National Security Agency surveillance, which Edward Snowden famously helped uncover a few years ago. The legal documents argue that apart from being a violation of the right to private speech, such surveillance also causes a “’chilling effect’, where a plaintiff responds to government action by ‘self-censoring’. Also, the information in the wrong hands carries the risk of profiling, that is, categorising people according to their habits, says Hickock.

Permission Granted

You would think that the government has no business legislating away our constitutionally guaranteed rights to live our lives privately, and anonymously. But haven’t we, in fact, already written off our right to remain private? And sometimes, even our friends’ rights? Just by downloading an app or connecting to a website, we are giving permission for an astonishing extent of access to data.

Last month, Truecaller, the app that looks to replicate the phone directory by accessing your contacts, launched new services. It will now be possible to know, who is available to take a call and who isn’t. Kari Krishnamoorthy, country manager of Truecaller India, explains in an email, “We have designed ‘availability’ to work without the need for you to do anything. We want to do all the hard work — so if you’re on a call or in a meeting, we automatically show you as ‘busy’ (with a red dot) to friends in your phonebook who use Truecaller.”

Sure, it does make life easier, keeping away unsolicited calls, but what this feature also does is tell someone when you are available but still not taking the call. (He confirms that the app does not track the ‘availability’ of a non-user). The app has over 100 million downloads, according to the Google Play Store: that’s 100 million people who have volunteered for Truecaller to keep and use data about their phone habits.

And it doesn’t help if you are not even a Truecaller user. The app will still get your information. The small print in its privacy policy says, ‘If you provide us with personal information about someone else, you confirm that they are aware that you have provided their data and that they consent to our processing of their data according to our privacy policy’. When quizzed about this concept of obtaining consent from somebody other than the owner of the information, Krishnamoorthy answered, “We do not want people to share the data of someone else if that person does not want his/her data to be shared”. Convenient argument, some would say.

But then, this is what the government too is doing through the Aadhaar Act. Section 8(2) says that a requesting entity (that is, any person or agency that wants to verify you from the Aadhaar database) must get your consent before collecting your identity information for authentication. An app, TrustID, already exists that purports to “verify your maid, cab-driver, tutor, carpenter and all other service providers using the Aadhaar ID’ in seconds. Does the app get permission from the person being verified? (Admittedly, the app pre-dates Section 8, but the basic privacy concern remains). An email sent to the app-makers on their official email address remained unanswered.

Small Print

Mihir Parikh, head of strategy and technology practice at law firm Nishith Desai Associates, reminds us that this practice of not reading 'terms of service' (ToS) is nothing new. He compares it with your bank account or insurance policy, for instance, which has pages of legalese in tiny font typically never read. Yet there is a difference. With a bank, the amount of data they access and control is limited. But, with apps, not only are you agreeing to ToS couched in the vaguest possible language, but also by living on your phone, they have access to virtually everything you do on it. Of course, you may have noticed that one of the permissions required by most apps typically say 'read the contents of your SD card' or 'modify or delete the contents of your SD card'. Once that is granted, there is no telling what an app is accessing or doing inside your phone, says Saket Modi, hacker and co-founder of security solutions company, Lucideus Technologies. He recommends working under the assumption that your phone is or will be hacked anyway.

Hobson's Choice

Facebook, one of the world's most valuable corporations, is notorious in the tech world for its privacy practices. For example, on the phone app, the section on privacy is just one click away on the drop-down. However, to realise that the company also collects information about your browsing even outside of Facebook, you will have to go to Privacy Settings–More settings–Ads-Manage The Preferences We Use To Show You Ads', where it reads: "That's why we have ad preferences, a tool, that lets you view, add and remove preferences we created for you based on things like your profile information, actions you take on Facebook and websites and apps you use off Facebook."

Even more importantly, the only say you have in this is to choose the type of ads that you see, not whether Facebook gets access to the rest of your off-Facebook Internet activities. That permission is, presumably, appropriated at the time you created your account. We asked Facebook about this practice, among other questions, but were told the company will not be 'participating' in the story.

The intrusion is compounded by the fact that a good number of Facebook users are people who signed into the service when the privacy policy was much less intrusive. The users, the foundation around which a 250 billion dollar empire has been built, have not been given any say in the matter, and are brushed off with the very familiar "Your continued use of the Facebook services, following notice of the changes to our terms, policies or guidelines constitutes your acceptance of our amended terms, policies or guidelines". One is left with a Hobson's choice — take it or leave it.

Many users share information under the false assumption that it won't be shared with any third parties or is only available for the consumption of their chosen friends, says Mishi Choudhary, legal director at Software Freedom Law Centre. She quotes Prof. Eben Moglen, a colleague at the Centre, to say that Facebook's focus on privacy controls is like that of a magician who waves a brightly coloured handkerchief in the right hand so that the left hand becomes invisible. "From a consumer's viewpoint, Facebook's fatal design error is not that Johnny can see Billy's data. It's that Facebook has uncontrolled access to everybody's data, regardless of the so-called 'privacy settings'. And even those users who adjust those settings can be surprised by where their information winds up," she says.

On Notice

In fact, a look through the ToS or privacy policies of companies can be quite entertaining. For example, Vonvon, a Korean company that makes quizzes on Facebook, has a privacy policy that says 'we do not share your personal information with third parties unless we have received your permission to do so, or given you notice thereof (such as by telling you about it in this privacy policy) or removed your name and any other personally identifying information from it…' To a lawyer, the portion in brackets suffices to authorise all sharing even without taking permission and without removing personally identifying information. Hyewon Cho wrote us from Vonvon to state: "We do not store any personal information what-so-ever regardless of ToS or Privacy policy, therefore no personal information to share in the first place".

The concern is compounded by the fact that in India, privacy laws barely exist, forget providing meaningful protection. "We must first have principles as to what is privacy and very specific laws as to what data is collected, who uses that data, and for what purpose," says Mishi Choudhary. "In addition, a proper law should provide for the right to see records about oneself, the right to request amendment of records that are not accurate, and the right of individuals to be protected against an unwarranted invasion of their privacy resulting from the collection maintenance and use of their personal information," she says.

Of course, that's still a long way off. Until then, caution is the only refuge. Saket Modi talks of the iCloud hacker who was recently arrested by the FBI for leaking nude pictures of world-famous celebrities. It turns out the hackers' modus operandi was simple. Send phishing emails to targets requesting them to share personal details, such as passwords, which they presumably complied with.

Vitali Kamluk, director - Global Research & Analysis, APAC, at Kaspersky Labs, explains it best. "Technology is a blackbox not only for common people but also for geeks. With the rise of advanced computer threats, no one can be assured that a device one is using is not compromised at a given point. Shall we be paranoid? Perhaps not. Shall we change our behaviour accordingly and be cautious while sharing personal data over the network? Yes, of course. Use your smartphone or tablet as if the whole world were watching you through the screen of your own device."

Provisions of Aadhaar Act, 2016

* "Benefit" means any advantage, gift, reward, relief, or payment, in cash or kind, provided to an individual or a group of individuals and includes such other benefits as may be notified by the Central government;
* "Service" means any provision, facility, utility or any other assistance provided in any form to an individual or a group of individuals and includes such other services as may be notified by the Central government;
* "Subsidy" means any form of aid, support, grant, subvention, or appropriation, in cash or kind, to an individual or a group of individuals and includes such other subsidies as may be notified by the Central government.

Section7

The Central government or, as the case may be, the state government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment.

The writer, a former Businessworld journalist, is currently an advocate, based in Delhi

This article was published in BW Businessworld issue dated 'May 2, 2016' with cover story titled *'Yes Bank-BW Best CFO Awards'*