Times of India Edition Delhi
7.5.2017 Page 20
Height 21.34cm Width 15.78 cm

Big Brother? 100 Small Brothers are watching you

SWAMINOMICS

SWAMINATHAN S ANKLESARIA AIYAR

The courts are hearing petitions against the government's expansion of schemes for which Aadhaar linkage is mandatory. Civil rights activists complain of privacy erosion, large-scale leakage of Aadhaar data, and violation of Supreme Court limits on Aadhaar. Some fear, rightly, that a premature insistence on Aadhaar can deprive poor people of welfare benefits: not all have Aadhaar numbers, and the telecom infrastructure is still woefully inadequate. The biggest fear is that Aadhaar's expansion will convert the government into George Orwell's 'Big Brother', watching your every move and robbing you of personal space.

Proponents of Aadhaar sneer that the activists are anti-technology Luddites, who unwittingly aid tax evaders and other crooks. These crooks can be caught by making Aadhaar mandatory for several purposes, producing data that helps catch the guilty.

However, this debate is irrelevant for the biggest privacy issue, which has nothing to do with Aadhaar. Privacy has mostly disappeared already with computers and cellphones being penetrated by hackers. Any misuse of Aadhaar pales in comparison with the misuse of viruses sitting on your computer or cellphone, watching all you say or write, and analysing this into behaviour patterns that even you may not realise.

The main threat to privacy does not come from giving access to your fingerprints and iris photos to the government. Immigration officials in dozens of countries routinely take your fingerprints and iris photos when you enter their airports, and passengers do not mind since this obviously helps track undesirables.

A top cybersecurity expert estimates that every email and phone call is monitored by at least a hundred invisible entities, of whom 52% are private actors and 48% are state actors (of more than one country). The state has no monopoly on snooping. Rather, states themselves are hacked daily. Despite spending billions on cybersecurity, states are losing this war. Far from governmental Big Brothers becoming all powerful monopolists of information, they themselves are leaking data and secrets like a sieve to foreigners and non-state actors. Privacy has disappeared for governments as well as individuals.

Russian hackers helped Donald Trump win the US presidential election by hacking into the Democratic Party's computers and releasing uncomfortable facts about Hillary Clinton. Hackers stole $101 million from the central bank of Bangladesh. In 2014, hackers called 'Guardians of Peace' leaked confidential data of Sony Pictures, including personal emails of employees and their families, copies of then-unreleased Sony films, and other information. The group demanded that Sony abandon its comedy film on a plot to assassinate North Korean leader Kim Jung-Un. Other hackers have stolen huge sums. Corporations buy leaked data for commercial gain. Criminals use leaked data for blackmail, theft, kidnapping and murder.

Thinkstock

PRIVATE SNOOPS: Every email and call is monitored by at least 100 invisible entities, of whom 52% are private actors

Countries and corporations with the most powerful anti-hacking systems have failed to protect themselves. What hope, then, is there for individuals?

The cybersecurity expert says that 70% of websites worldwide are compromised. Daily checks are no defence: it can take 240 days for experts to detect a hack. Viruses are growing by 66% per year, some aiming to watch and record, others aiming to destroy systems. They can see every financial transaction, every compromising revelation in emails and phone calls, every movement of you and your family.

Cyberspace is a global commons that defies regulation. Anybody can enter it and penetrate systems globally. Not all hackers are criminals or corporations seeking commercial data: some seek to do good by exposing facts (like WikiLeaks).

Through history, states have been powerful and individuals powerless. States were therefore the main threats to civil liberties and privacy. But increasingly non-state actors (notably ISIS and the Taliban) can threaten and overwhelm states. Tax evaders, money launderers and drug traffickers remain untouched by the most powerful states.

Civil rights activists say little or nothing to the threat to privacy from private actors. Yet these threaten both privacy and security, and governments need additional powers to deal with hackers as well as criminals. Data mining is a powerful tool that helps governments detect tax evaders, blackmailers, terrorists, and other undesirables who escape the traditional police system. Governments must beef up cybersecurity, for itself and citizens. Making Aadhaar leakproof is only a small part of that.

India needs a Privacy Act, not just to check excesses in government snooping but to guard against private snooping. When civil rights are being breached massively by undesirable private actors of all sorts, to focus on government misuse alone — as activists are doing — is myopic.