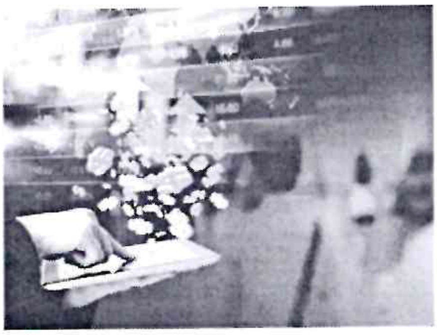
Alun

India's data localisation push can give rise to new business opportunity

By Shelley Singh, Dinesh Narayanan, ET Bureau | Updated: Oct 25, 2018, 08.12 AM IST

1 Comments



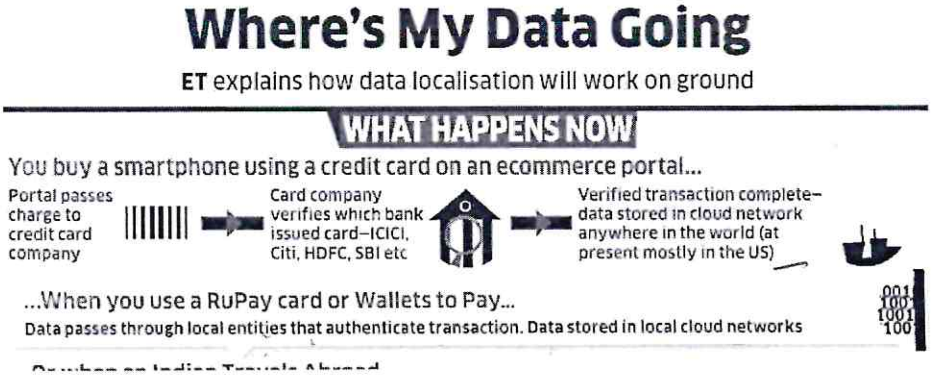
By 2050, India will be at number 5 spot in size of data centre market.

No one has ever doubted the sheer consumerism of Indian festivity, but its presence reaches further than you would believe. For, all that data on what smartphones or shirts, boots or white goods that we buy and how we pay for it, rarely stays on our shores.

This week's festive season sales may generate online business of up to $3 billion. But much of the data from those sales, on ecommerce platforms and more, is likely to be hosted and stored in US data farms. While this has been happening since the start of online shopping and even earlier, this time, Reserve Bank of India (RBI) has firmly stated that all financial transactions' data must be locally stored.

This is driving data centre infrastructure spending, which could touch $4.5 billion by end of 2018 and $7 billion by 2020, according to real estate consultant Cushman & Wakefield's blog on data centre growth in India. In fact, research and advisory firm Gartner sees data centre hardware spend alone to be $2.7 billion by 2018. India had built up data centre infrastructure of 1.3 million square feet in 2008, expected to scale to 10.9 million sq feet by end of 2018, says Cushman & Wakefield. By 2050, India will be at number 5 spot in size of data centre market.

This explosion will be driven by localisation and backed by clichés — data is the new oil, why should data of over one billion Indians not be in India, data is strategic and foreign entities could cripple India in event of war or sanctions, how will Indian law enforcement go after data gangs in Macau, Moscow, Madrid or Manhattan if systems are compromised and so on.



Where's My Data Going

ET explains how data localisation will work on ground

WHAT HAPPENS NOW

You buy a smartphone using a credit card on an ecommerce portal...

Portal passes charge to credit card company

Card company verifies which bank issued card—ICICI, Citi, HDFC, SBI etc

Verified transaction complete—data stored in cloud network anywhere in the world (at present mostly in the US)

...When you use a RuPay card or Wallets to Pay...

Data passes through local entities that authenticate transaction. Data stored in local cloud networks

SPOTLIGHT

Global Watch

Ghosn exit sets stage for Renault-Nissan future clash

An alliance meeting is planned for next week in Amsterdam, that may include Daimler, said a person with knowledge of the matter.

- In era of online retail, Black Friday still lures a crowd
- United States asks allies to shun Huawei equipment

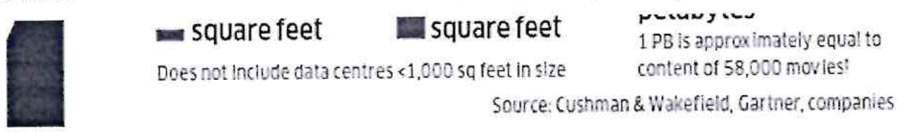
Most Read Most Shared Most Commented

Experts say Twitter CEO Jack Dorsey's placard faux pas could cost company dear

Delay in government spends hurts IT companies' revenues

IIT-Kharagpur develops tech to filter fake news about disasters

Indian IT industry is making convincing strides as their clients demand digital transformation



Source: Cushman & Wakefield, Gartner, companies

A chief information officer of a multinational manufacturing firm, which has been keeping Asia Pacific enterprise data in India for the past four years, says it saved 30-40 per cent in costs. India is an ideal location for lower cost of operations, availability of quality talent and round-the-clock service, he says.

B Srinivasa Rao, chief marketing officer, CtrlS Datacentres, which runs Asia's largest tier IV data centres in Hyderabad, Mumbai and Gurgaon, says many ecommerce and fintech clients see India as a cost saver. The manpower, real estate and bandwidth costs come down by about 80 per cent compared to a top-tier data centre in the US or Singapore. Imran Iraqi, principal, financial technology services, CtrlS, believes it will continue to grow at the same pace over the next five years.

CtrlS is spending Rs 1,500 crore on setting up hyperscale data centres in Hyderabad and Mumbai, which would require about 100MW and 50MW, respectively. NetMagic, acquired by Japan's NTT Com in 2012, has nine data hosting facilities in India, two of which were set up early this year at an investment of $144 million. Flipkart's PhonePe and Alibaba-backed Paytm claim their transactions are processed locally.

Siddharth Vishwanath, partner, cybersecurity, PwC India, says, "Global companies will need to invest more in infrastructure development and re-architect the way applications work." He points out that companies such as Google Pay, which have a common global data backbone for multiple countries, will also need a separate one for India to comply with local regulations.

Types of Data Clouds

Data centres are certified by the Telecommunication Industry Association (TIA) of the US according to their efficiency and uptime:

Tier I-II

Old and used by small set-ups that do not suffer much if services are down for a few hours or even days

Tier III

99.982% uptime a must

Tier IV

99.995% uptime mandatory

Caters to critical infrastructure and services – such as banking and power utilities – that cannot afford even a few minutes' disruption crucial to our economic partnership," they wrote on October 12.

Echoing the sentiment, Mukesh Aghi, chief executive, US India Strategic Partnership Forum (USISPF), says the forum supports free flow of data and opposes forced data localisation. USISPF is a trade body representing US corporates in India, such as Visa, MasterCard. Amex, Amazon and Western Union, among others.

"We expect these requirements (of local centres) to raise cost of procuring and delivering services, including for local Indian businesses, which will ultimately increase costs and reduce availability of data-dependent services."

1
Comments

Read more on Rbi Data Localisation Data Centres India Data Localisation India Data Localisation Data Centres

Also Read

Alibaba backs data localisation in India

All about India's data localisation policy

Data localisation: The Reserve Bank of India stands firm

RBI sticks to October 15 deadline for data localisation

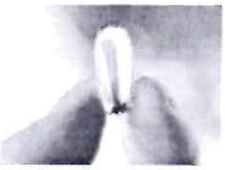
Law enforcement agencies favour data localisation

Comments (1) Add Your Comments

Recommended For You

Sponsored by

These Twin-Level Penthouses are starting R...
Ad: Satya Group



Men, you don't need the blue pill if you do this once...
Ad: Testo Ultra

Promote your content on 100+ premium sites
Ad: Colombia

Boost your potential.Choose from our career-defining...
Ad: Symbiosis

India in spotlight as global central banks battle...

Consultations on ecommerce policy to start...

Outgoing information commissioner defends his...

India may get its first-ever woman CEA

Get a Quote

Type Company Name

Browse Companies

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z | 1 2 3 4 5 6 7 8 9

Browse Mutual Funds

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Powered by

Live Market
News
Portfolio
Mobile
Live TV

Industry
Newsletters
Commodities
Speed
Blogs

About Us
Subscribe to ET Prime
Book your Newspaper Subscription
Create Your Own Ad
Advertise with Us

Extract and analyse: Cops target suspects' cloud data

AIMING FOR THE CLOUD

Cloud Analysis software will allow Delhi Police to scan virtual storage space of suspects

Why

- Companies and individuals fast switching from traditional hard-drive storage to cloud-based services
- A criminal investigation requires police to obtain data for analysis
- Mostly, the data is encrypted or locked

What Delhi Police is looking to extract from cloud-based storage

Files in form of pictures, videos, text, zip and many other formats

Features of the software

Cloud sources | Google Drive/ Google Plus/ Apple- iCloud

Cloud services | Dropbox, Flickr, Google Drive, SkyDive, OneDrive, Yandex

Operating systems | Windows, Mac OS X, Unix, iOS, Android, Windows, Blackberry

Peer-to-peer software | Area Galaxy, eMule, Frostwire, Gigatribe, Shareaza, Torrent

Messengers | Tango, Telegram, Text Plus, TextMe, Viber, WeChat, WhatsApp, Snapchat

Rajshekhar.Jha
@timesgroup.com

New Delhi: Delhi Police is gearing up to acquire a technology that will allow it to hack into cloud-based storage systems of suspects and extract data for analysis. Sources said that the programme would be used by Special Cell's cyber unit as well as the economic offences wing during investigation.

The police department denied that the objective of this procurement was to snoop. Senior officials clarified that this software will only be used to access encrypted and locked data stored on clouds by individuals and companies under investigation.

"This programme is called the Cloud Analysis software, which will not hack into any random cloud storage but will be restricted to devices and accounts related to a particular investigation," an officer said. Another source said that the software will be installed in the mobile cyber crime forensic lab of the EOW unit.

The department has been carrying out investigation using the available extraction programmes that could analyse and scan data from the hard disks of the suspects' computers and laptops. The software could make a mirror image of the disk, which could then be sent for forensic analysis.

However, the need for this new technology has been felt in the wake of suspects resorting to saving data on clouds to escape surveillance. This has apparently come to fore in several probes conducted by police in the recent past.

This change in modus operandi, sources say, has made the police's job tougher as it also takes away a crucial piece of evidence collection, i.e. seizures. With cloud systems in place, the police may not get an opportunity to seize a hard disk belonging to an accused and will have to officially access the cloud data and get it verified by the forensic department.

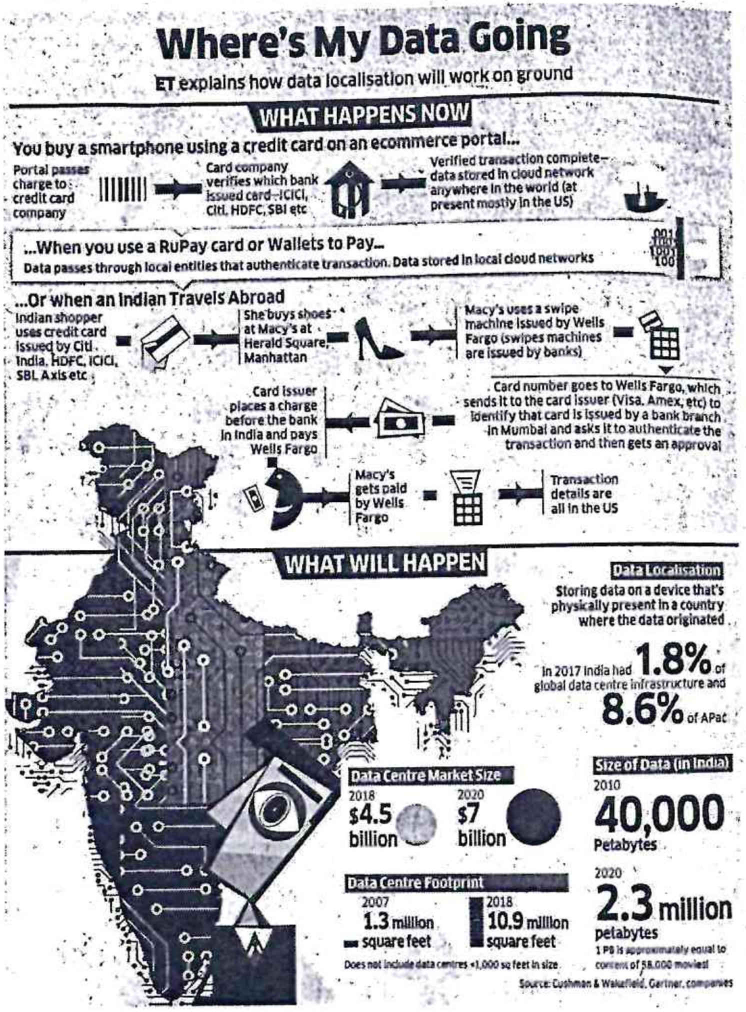
The software that Delhi Police is looking to procure will be able to extract data from Google drives as well as Apple's iCloud. The cops are hoping that the programme will also allow them to access cloud services like Dropbox, Flickr, SkyDive and OneDrive, etc.

This will work on most computers as well as mobile operating systems and detect files in the form of text, music, videos or pictures, apart from compressed files. "The programme will be able to scan through a range of email clients, browsers, MS Office files and peer-to-peer software as well. Chat files, which help in building cases against the accused most of the times, can be explored as well. Apart from common chat platforms, the system will also be able to read chat logs on platforms like Text Plus, Textie, Tango and Telegram, the officer said, quoting a document.

aters and high-pressure zones have long production are more expensive than in, business is capital intensive, involving Former director (offshore), ONGC But low crude prices in the last three rich in all these efforts

Data Checks In

With RBI not budging on financial data localisation and the government finalising the data bill, a new business opportunity is set to explode. **ET** takes a look at how data will make money and how localisation will work on the ground



Where's My Data Going

ET explains how data localisation will work on ground

WHAT HAPPENS NOW

You buy a smartphone using a credit card on an ecommerce portal...

Portal passes charge to credit card company → Card company verifies which bank issued card—ICICI, Citi, HDFC, SBI etc → Verified transaction complete—data stored in cloud network anywhere in the world (at present mostly in the US)

...When you use a RuPay card or Wallets to Pay...

Data passes through local entities that authenticate transaction. Data stored in local cloud networks

...Or when an Indian Travels Abroad

Indian shopper uses credit card issued by Citi India, HDFC, ICICI, SBI, Axis etc → She buys shoes at Macy's at Herald Square, Manhattan → Macy's uses a swipe machine issued by Wells Fargo (swipes machines are issued by banks)

Card number goes to Wells Fargo, which sends it to the card issuer (Visa, Amex, etc) to identify that card is issued by a bank branch in Mumbai and asks it to authenticate the transaction and then gets an approval → Card issuer places a charge before the bank in India and pays Wells Fargo

Macy's gets paid by Wells Fargo → Transaction details are all in the US

WHAT WILL HAPPEN

Data Localisation

Storing data on a device that's physically present in a country where the data originated

In 2017 India had **1.8%** of global data centre infrastructure and **8.6%** of APac

Data Centre Market Size

2018 **$4.5 billion**

2020 **$7 billion**

Size of Data (in India)

2010 **40,000 Petabytes**

2020 **2.3 million petabytes**

1 PB is approximately equal to content of 58,000 movies!

Data Centre Footprint

2007 **1.3 million square feet**

2018 **10.9 million square feet**

Does not include data centres <1,000 sq feet in size

Source: Cushman & Wakefield, Gartner, companies

Shelley Singh & Dinesh Narayanan

No one has ever doubted the sheer consumerism of Indian festivity, but its presence reaches further than you would believe. For, all that data on what smartphones or shirts, boots or white goods that we buy and how we pay for it, rarely stays on our shores.

This week's festive season sales may generate online business of up to $3 billion. But much of the data from those sales, on ecommerce platforms and more, is likely to be hosted and stored in US data farms.

While this has been happening since the start of online shopping and even earlier, this time, Reserve Bank of India (RBI) has firmly stated that all financial transactions' data must be locally stored.

This is driving data centre infrastructure spending, which could touch $4.5 billion by end of 2018 and $7 billion by 2020, according to real estate consultant Cushman & Wakefield's blog on data centre growth in India. In fact, research and advisory firm Gartner sees data centre hardware spend alone to be $2.7 billion by 2018. India had built up data centre infrastructure of 1.3 million square feet in 2008, expected to scale to 10.9 million sq feet by end of 2018, says Cushman & Wakefield.

By 2050, India will be at number 5 spot in size of data centre market.

This explosion will be driven by localisation and backed by clichés — data is the new oil, why should data of over one billion Indians not be in India, data is strategic and foreign entities could cripple India in event of war or sanctions, how will Indian law enforcement go after data gangs in Macau, Moscow, Madrid or Manhattan if systems are compromised and so on.

Kartik Shinde, partner, cybersecurity, EY India, says, "If the end beneficiary is in Macau, where there are a lot of casinos, you have to liaise with lawyers in Macau. That's easier said than done. Fraudsters (in and outside India) study the system and number of hops (number of countries and banks it goes via) say for money transfer, and devise the best way to defraud."

DRIVING EFFICIENCY

The benefits are obvious. Rakshit Daga, vice-president, engineering, BigBasket, says, "It will speed up transactions and reduce network latency." When the online grocery store shifted its data centre (hosted on Amazon Web Services) from Singapore to Mumbai, it noticed up to 10% improvements in transaction efficiency. "Shifting from the US to India could lead to up to 30% better speeds," he adds.

A chief information officer of a multinational manufacturing firm, which has been keeping Asia Pacific enterprise data in India for the past four years, says it saved 30-40% in costs. India is an ideal location for lower cost of operations, availability of quality talent and round-the-clock service, he says.

B Srinivasa Rao, chief marketing officer, CtrlS Datacentres, which runs Asia's largest tier IV data centres in Hyderabad, Mumbai and Gurgaon, says many ecommerce and fintech clients see India as a cost saver. The manpower, real estate and bandwidth costs come down by about 80% compared to a top-tier data centre in the US or Singapore. Imran Iraqi, principal, financial technology services, CtrlS, believes it will continue to grow at the same pace over the next five years. CtrlS is spending ₹1,500 crore on setting up hyperscale data centres in Hyderabad and Mumbai, which would require about 100MW and 50MW, respectively.

NetMagic, acquired by Japan's NTT Com in 2012, has nine data hosting facilities in India, two of which were set up early this year at an investment of $144 million.

Flipkart's PhonePe and Alibaba-backed Paytm claim their transactions are processed locally.

Siddharth Vishwanath, partner, cybersecurity, PwC India, says, "Global companies will need to invest more in infrastructure development and re-architect the way applications work." He points out that companies such as Google Pay, which have a common global data backbone for multiple countries, will also need a separate one for India to comply with local regulations. "Data is a digital transactions footprint. During war or hostilities, data centres could be switched off. Such scenarios, among others, are pushing countries towards local infrastructure," he adds.

Types of Data Clouds

Data centres are certified by the Telecommunication Industry Association (TIA) of the US according to their efficiency and uptime:

Tier I-II

Old and used by small set-ups that do not suffer much if services are down for a few hours or even days

Tier III

99.982% uptime a must

Tier IV

99.995% uptime mandatory

Caters to critical infrastructure and services – such as banking and power utilities – that cannot afford even a few minutes' disruption

Data centres must be plugged into two power grids – that is, state and national in case of India

Some miss tier IV classification simply because fallback power supply is an onsite diesel generator

TIA-942 standard annual downtime limit

Tier I	<28.8 hours
Tier II	<22 hours
Tier III	< four hours
Tier IV	< 24 minutes

Even when an Indian user shops at Macy's in New York on an Indian bank's credit card, transactions may be routed via Wells Fargo (which issues card swipe machines to Macy's) in the US and stored there rather than in India (**See graphic**).

MIRROR, MIRROR ON THE WALL

Some companies are insisting on mirroring rather than storing information only in India. Earlier this month, WhatsApp said it has built a system to store payments-related data locally in India through mirroring. "We hope to expand WhatsApp payments to all of India soon so we can contribute to financial inclusion goals," a company statement noted.

But mirroring has not cut ice. "It's like a photocopy. The original will be outside India. Mirroring is not good enough," says Shinde of EY India. Vishwanath adds, "Mirroring is a subset. The regulator is stating that data cannot go out, so mirroring is not a solution."

The banking regulator is insisting on hard localisation by October 15, though global payments companies have been lobbying with the finance ministry and RBI for relaxation. Some have sought a year's extension but to no avail so far.

Among reasons for local hosting are ease of access for law enforcement and privacy. However, Prashant Pradhan, vice-president, IBM Asia Pacific, says, "Physical location does not eliminate need for protocols and permissions to access. Situations (like sanctions or war) might be driving intent, but access is not controlled by the Government of India but by the owner."

Global tech and payments giants consider forced localisation against the grain of free trade and data flow. In a strongly-worded letter to Prime Minister Narendra Modi, US Senators John Cornyn and Mark Warner — co-chairs of the Senate's India caucus that comprises over 30 members — urged India to instead adopt a "light touch" regulatory framework that would allow data to flow freely cross-border.

"We see this as a fundamental issue to further development of digital trade and one that is crucial to our economic partnership," they wrote on October 12.

Echoing the sentiment, Mukesh Aghi, chief executive, US India Strategic Partnership Forum (USISPF), says the forum supports free flow of data and opposes forced data localisation. USISPF is a trade body representing US corporates in India, such as Visa, MasterCard, Amex, Amazon and Western Union, among others.

"We expect these requirements (of local centres) to raise cost of procuring and delivering services, including for local Indian businesses, which will ultimately increase costs and reduce availability of data-dependent services."

Scanned with CamScanner

From Aadhaar to data localisation to information privacy, next year will see big shift in big tech

Going Out on a Big Date with Big Data

T K ARUN
Editor, Opinion

Countless numbers of retail outlets and offices today sport an electronic box with a patch that glows deep green. Employees mark their attendance by pressing a finger on that unfaltering green eye. An increasing number of smartphones offer 'face unlock' as a standard feature: the phone has software that can be trained to recognise the owner's face and unlock the phone on seeing the face. Less fancy ones recognise fingerprints.

Banks and credit card companies let you authenticate yourself using your voice when you call their helpline. Some airports are gearing up to do away with boarding passes, letting facial recognition software do the job for you — it is standard practice at some Chinese terminals. Police routinely identify culprits from the footage of surveillance cameras that record and store whatever transpires under their watch.

Then, of course, there are Google and Facebook, who know everything about you, because you happily shovel that information to them without their having to ask.

Bank and credit card statements populate your Gmail, besides your medical reports and travel bookings. Your calendar helps you plan your life, but also reveals to Google what you do, whom you meet and where. Google Maps tracks your movements with far greater aplomb and accuracy than an anxious mother can muster in relation to her teenaged daughter. Your search and browsing history, including on Youtube and whatever else you watch logged into the Chrome browser, reveal more about you to Google than what you tell your therapist.

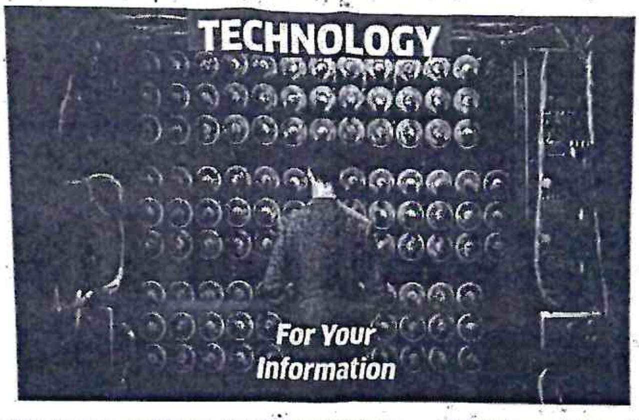
Facebook's idea of what you actually like is hazy. Eagerness to be liked and not offend makes most people 'like' many things on Facebook that they might be indifferent to, if not actually abhor. But Facebook certainly knows who your friends are, who their friends are, what they wear, what they do, where they go and what their major transitions in life are. Facebook also owns WhatsApp, India's favourite messaging app. But Facebook claims ignorance of the contents of its messages.

Amazon, of course, knows the exact shade of your consumerist hedonism. Bookmyshow, Netflix and Amazon Prime know the movies you watch and can probably draw your psychological profile. Swiggy and Zomato know what gives you your umami and how much you are willing to pay for it. Your payment wallets and card companies analyse your spends before you ask for it.

Your smartphone is loaded with apps that seek and obtain permission to access your contacts and messages, scan your photographs and inherit 1% of your estate when you die. (Can you put your hand on your heart and swear they don't?)

The long point is that a host of private companies collect, store and act on a whole lot of your personal data. Your gut bacteria own your mood and level of sanity. Collectors of your data dictate your conduct, leaving some tiny room, we hope, for god, spouse and conscience, acting jointly or severally.

The short point is that data protection is not just about Aadhaar.



Most Indians now possess the 12-digit unique identity (UID) number and have linked it to bank accounts, telephone numbers and their income tax Permanent Account Numbers (PAN). The trouble is, a whole lot of other Indians, besides the designated authority in charge of Aadhaar, also possess at least the Aadhaar numbers and demographic details of their countrymen, if not their biometric data. Time and again, state government departments have put out list of beneficiaries of assorted state schemes, complete with Aadhaar numbers. The Tribune reported a major breach in Aadhaar's link to the agencies across the country that enrolled members, which allowed some entrepreneurs to sell Aadhaar details to anyone willing to pay Rs 500.

The Unique Identity Authority of India (UIDAI) has responded with a scheme of virtual Aadhaar numbers that are dynamically generated and stay valid for a limited period for a limited purpose. This is a good solution, but does not address the loss of ID number privacy lost in previous data breaches.

Ideally, the UIDAI should issue fresh Aadhaar numbers to all previous allottees, and continue with virtual numbers based on the new set of numbers. This would be administratively difficult and expensive, but it should be done to secure Aadhaar, which is a valuable tool of governance.

Shoddy, leaky enrolment is not the only problem with Aadhaar. Its legal basis for use by non-State entities got knocked down by the Supreme Court. As of now, Aadhaar can be used only for the purpose of channelling government funds to beneficiaries, besides for taxpayer identification.

This is the result not of Supreme Court judges' inability to appreciate the immense benefit Aadhaar has brought to microfinance companies and their millions of customers. Or Aadhaar's empowerment of migrant workers in lands far away from home, enabling them to establish their identity and secure a bank account and a phone connection. The problem is twofold: one was GoI's sleight of hand, of getting the Aadhaar law passed by Parliament as a money Bill that bypassed Rajya Sabha; and the other was its failure to put in place, before legislating on Aadhaar, a well thought-out data protection law.

The coming year will see these problems getting fixed. A proper data protection law will have to be enacted, seeking consensus rather than strong-arm measures of the kind that rammed the Aadhaar Bill through Parliament. Aadhaar will have to be enacted afresh, shielded by a strong data protection law and shedding the tag of a money Bill.

The judges who said that GoI could justify passing the Aadhaar Bill as a money Bill then felt constrained to limit the use of Aadhaar to matters related to government monies. That constraint has to go, to enable private parties to use Aadhaar-Based Biometric Authorisation (ABBA). ABBA is a key enabler for the deprived sections of society. To bring it back, the safest, surest method is to pass Aadhaar afresh, passing it through both Houses of Parliament.

400.76 million
Subscribers have changed their operator since mobile number portability was introduced

A key question in data protection is data localisation. Should data on Indians be stored in India and exclusively in India? The case for storing it in India is strong. India is a large enough data generator for Indian data to be stored in India without worrying about losing economies of scale. Local storage would ensure availability of Indian data for judicial purposes.

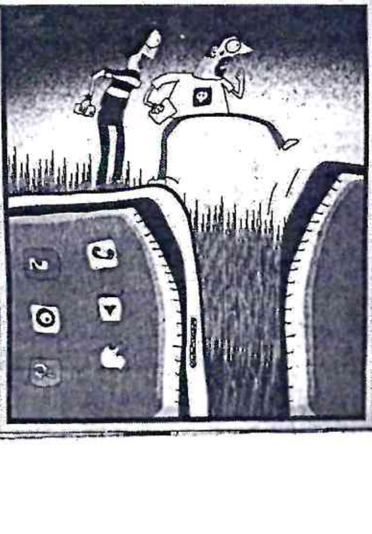
Local storage would likely create fresh business for the Cloud arms of Amazon, Google, Microsoft and IBM. As a major provider of data based services around the world India has to be mindful of data rights and reciprocity requirements of other jurisdictions, when deciding on exclusive storage of Indian data within India.

Making the data stored in India available to companies creating artificial intelligence (AI) is another key challenge. AI depends on training algorithm on data.

Working these out cannot be rushed. A thorough legal framework for data protection and data sharing cannot be undertaken by a lame duck government. A coalition government, whose senior partner is called a thief by its junior partners with impunity and lacks a majority in the Upper House, to boot, is lame, even if it does not quack. We will have to wait for the elections to be over, to put digital India on a secure footing.

Techtonic Shift

Consumers will be taking a big leap in data consumption, fundamentally changing the business of data crunching



1.17 BILLION
Number of mobile phone subscribers now – about 2.5 times the level (457 m) nine years ago

THE GREAT DATA HEIST

Data is said to be the new oil. It's hardly surprising that criminals are increasingly targeting this new-age, valuable commodity through cyber attacks, the latest being the data breaches at the Marriot Hotels and Quora. Here's a look at the biggest attacks, the cost and the reasons behind them

y Indulekha Aravind

196 days The average time it takes an organisation to detect a breach

$148 The average cost of a data breach per compromised record

What is a Data Breach?

A data breach happens when information is accessed without authorisation

$39.5 million Cost of a mega breach involving 1 million compromised records

$350.5 million Cost of a breach involving 50 million records

$3.9 million Average cost of global data breaches in 2018

Locations which saw the most expensive data breaches

US • Middle East • Canada

Source: A 2018 "Cost of a Data Breach" study by the Ponemon Institute, IBM

A Verizon Study Reveals that in 2018 There Were

53,308 security incidents

2,216 confirmed data breaches

Across 65 countries

73% cyber attacks were perpetrated by outsiders

76% of breaches were financially motivated

Data breaches can occur due to a variety of reasons, including

- Out-of-date software
- Weak passwords
- Targeted malware attacks

Attacks in India

$10.3 mn Average economic loss incurred by a large organisation in India because of cyber attacks, according to a Frost & Sullivan study

Poor investment in high-end security solutions

It is the big reason Indian organisations are more susceptible to data breaches, according to a report, M-Trends-2016. Few organisations, it said, have move beyond antivirus software to detect malicious mechanisms across an entire area.

Zomato

Detected in May 2017

IMPACT 17 mn users

Records of about 17 million users of Zomato were compromised in a security breach, the company revealed in May 2017. Names, email addresses and passwords were taken from its database.

FreshMenu

Detected in Sep 2016

IMPACT 110,000 users

Food delivery startup FreshMenu was the victim of a massive data breach, which exposed data of over 110,000 customers including names, email addresses, phone numbers, home addresses, device information and order history.

ATM Hacked

October 2016

IMPACT 3.25 mn debit c

Around 3.25 million debit cards were at risk when data was stolen from th private bank ATMs serviced by Hita Payment Services. The cards include 2.65 million of Visa and MasterCard 600,000 of RuPay.

Source: Cisomag.com; Ponemon I Verizon; IBM

Major Data Breaches in the 21st Century

Marriott Hotels

IMPACT 500 million clients

WHEN November 2018

The data of up to 500 million guests who booked reservations at its Starwood properties are believed to have been compromisedThe compromised information includes names, mailing addresses, phone numbers, email addresses, passport numbers and Starwood Preferred Guest account information. The chain is now facing multiple lawsuits by customers.

Quora

IMPACT 100 million users

WHEN December 2018

The website Quora reported that hackers stole the data of around 100 million users, which could include name, email address and an encrypted version of their password.

Facebook

IMPACT 30 million users

WHEN Detected in Sep 2018

In September, hackers used a flaw in Facebook's "view as" feature to gain unauthorised access to millions of accounts. Access tokens for 30 million accounts were stolen by hackers, who accessed contact information (name and email id/ phone number) for 14 million accounts, and additional information including gender, religion, location, device information and the 15 most recent searches for another 15 million accounts.

Yahoo

IMPACT 3 billion users

WHEN Detected in Sep 2016

In September 2016, Yahoo said it had been the victim of the biggest data breach yet, likely by "a state-sponsored actor" in 2014. The attack compromised the names, email addresses, dates of birth and telephone numbers of 500 million users. In December 2016, it said a breach in 2013 had compromised 1 billion accounts. In 2017, Yahoo revised that estimate to all 3 billion of its user accounts

Adult Friend Finder

IMPACT Over 400 million accounts

WHEN Detected in Oct 2016

Hackers collected 20 years of data, including names, email addresses and passwords of those who used adult content sites like Adult Friend Finder and Penthouse.

Uber

IMPACT 57 million users & 600,000 drivers

WHEN Late 2016

Uber found that hackers got names, email addresses and mobile phone numbers of 57 million users of its app. They also got the driver licence numbers of 600,000 Uber drivers. Uber made the breach public only a year later. They also paid the hackers $100,000 to destroy the data, though it could not verify that it was done.

Target Stores

IMPACT 110 million customers

WHEN Detected in Dec 2013

Hackers gained access to Target's point-of-sale card readers, and collected about 40 million credit and debit card numbers. This was revised to information of 70 million customers, and then 110 million. Its CIO resigned in March 2014. The cost of the breach was estimated at $162 million.

Lawsuit in US adds to Facebook's troubles over data protection

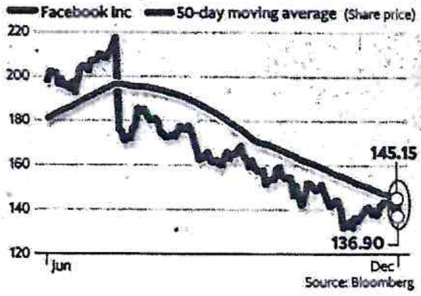
Suit seeks injunction 'to ensure Facebook puts in place protocols and safeguards to monitor users' data'

AFP
feedback@livemint.com
WASHINGTON

MINT GRAPHITI

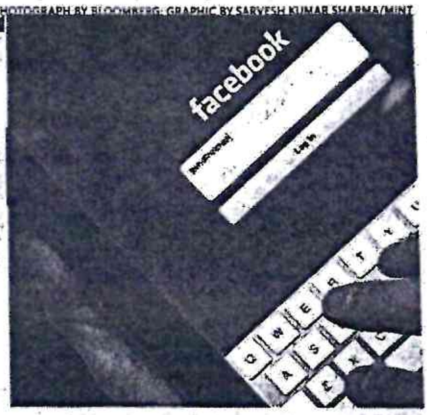
Facebook slumps

The stock has dropped 40% since July



Source: Bloomberg

PHOTOGRAPH BY BLOOMBERG; GRAPHIC BY SARVESH KUMAR SHARMA/MINT



'Facebook leaked data to consultancy working on Trump campaign'

The suit alleged that Facebook leaked data to a consultancy working on Donald Trump's 2016 campaign

Lawsuit is about making Facebook live up to its promise to protect users privacy, read AG's statement

Facebook responded: 'We're reviewing the complaint and look forward to continue talks with AG in DC'

Facebook shares ended the trading day down 7.25% to $133.24 and slipped lower in after-market trades

Facebook's woes mounted Wednesday as it faced a lawsuit alleging privacy violations related to data leaked to a consultancy working on Donald Trump's 2016 campaign, and as a new report suggested it shared more data with partners than it has acknowledged.

Facebook shares already sagging under the weight of the social network's troubles ended the trading day down 7.25% to $133.24 and slipped even lower in after-market trades. The suit filed by the attorney general (AG) for the US capital Washington is likely the first by an official US body that could impose consequences on the world's leading social network for data misuse.

"Facebook failed to protect the privacy of its users and deceived them about who had access to their data and how it was used," said attorney general Karl Racine in a statement.

"Facebook put users at risk of manipulation by allowing companies like Cambridge Analytica and other third-party applications to collect personal data without users' permission. Today's lawsuit is about making Facebook live up to its promise to protect its users' privacy." The suit filed in Superior Court in Washington seeks an injunction "to ensure Facebook puts in place protocols and safeguards to monitor users' data and to make it easier for users to control their privacy settings," and demands "restitution" for consumers.

Facebook said: "We're reviewing the complaint and look forward to continuing our discussions with attorneys general in DC and elsewhere." The social network has admitted that up to 87 million users may have had their data hijacked by Cambridge Analytica, which shut down weeks after the news emerged on its handling of private user information.

The suit seeks a ruling 'to ensure Facebook puts in place protocols to monitor users' data', restitution for consumers

A whistle-blower at the consultancy, which worked on Trump's presidential campaign, said it used Facebook data to develop profiles of users who were targeted with personalized messages that could have played on their fears. The scandal has triggered a series of investigations and broad review by Facebook on how it shares user data with third parties.

The New York Times reported that some 150 companies—including powerful partners like Amazon, Microsoft, Netflix and Spotify—could access detailed information about Facebook users, including data about their friends.

According to documents seen by the *Times*, Facebook allowed Microsoft's Bing search engine to see names of Facebook users' friends without consent and gave Netflix and Spotify the ability to read private messages. The report said Amazon was able to obtain user names and contact information through their friends, and Yahoo could view streams of friends' posts. While some of the deals date back as far as 2010, the *Times* said they remained active as late as 2017—and some were still in effect this year. "It appears that Facebook has not been honest with Congress or the public about how it treats its users' data," Congressman Frank Pallone, a Democrat, said in a tweet.

Facebook's head of developer platforms and programs, Konstantinos Papamiltiadis, said in a blog post that the *Times* report referred to partnerships that enabled "social experiences—like seeing recommendations from their Facebook friends—on other popular apps and websites." None of those partnerships or features "gave companies access to information without people's permission," he said, adding that the deals did not violate a 2012 privacy settlement with the US Federal Trade Commission. Papamiltiadis said, however, that "we've been public about these features and partnerships over the years because we wanted people to actually use them." But he said most of the features are now gone.

Netflix said that the feature was used to make the streaming service "more social" by allowing users to make recommendations to friends, but that it stopped using it in 2015. "At no time did we access people's private messages on Facebook or ask for the ability to do so," Netflix said in a statement.