GLOBAL RISK MANAGEMENT INSTITUTE

CREATING
RISK INTELLIGENT PROFESSIONALS

GRMI | GLOBAL RISK MANAGEMENT INSTITUTE

Data Privacy | by Govind Kumar (Batch 6)

PROGRAMME ENDORSED BY	ASSOCIATE PARTNER	STRATEGIC PARTNER	ASSOCIATE MEMBER	STRATEGIC PARTNER
othm qualifications	The Institute of Internal Auditors India	SHRM BETTER WORKPLACES BETTER WORLD	FICCI Federation of Indian Chambers of Commerce and Industry	HAUSPETER Consulting Internal Auditing Control

What is Data Privacy?

Data privacy or information privacy is a branch of data security concerned with the proper handling of data – consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around:

Whether or how data is shared with third parties.
How data is legally collected or stored.
Regulatory restrictions such as GDPR, HIPAA, GLBA, or CCPA.

No Such Law In India

Security incidents related with Personal Data

indianexpress.com/article/explained/explained-how-big-is-the-bigbasket-data-breach-7026688/

The Indian EXPRESS Home India World Cities Opinion Sports Entertainment Lifestyle Tech Video

Written by **Pranav Mukul** , Edited by Explained Desk | New Delhi | Updated: November 12, 2020 9:52:49 am

EXPRESS explained. SCI-TECH

bigbasket

Cyble has claimed that personal information of as many as 20 million users such as full names, email IDs, password hashes, etc

India's top online grocer BigBasket has suffered a potential data breach **resulting in personal information of over 20 million customers** being allegedly sold on the dark web. This incident follows a series of data breaches that have impacted Indian companies.

Waiting for secureapps...

- **Banking:** In January 2019, an SBI server in Mumbai was shown to be unsecured and vulnerable, exposing the data of **millions of its customers**. The server was not password protected, and so information such as account balances, mobile numbers, and even account numbers were effectively on display. SBI secured the server soon afterwards, but this incident emphasised the need for improving digital infrastructure in the banking sector.

- **Aadhaar:** The World Bank and certain digital security firms reported that in 2018 the Aadhar data of citizens was being sold online, with almost **a billion users being affected** in just the first few months of 2018. These leaks were a mixture of overt hacks and unprotected servers or leaky government websites. For example, in 2019 the Jharkhand government's website displayed the Aadhar details of around 100,000 government workers.

- **Whatsapp Pegasus:** In 2019, it was reported the Israeli firm NSOs software *Pegasus* was being used **to spy on 19 individuals**, including journalists and human rights activists. By hacking into their devices via a simple missed call, the attackers gained complete access to the individual's data, including locations, passwords, and even the ability to turn cameras and microphones on.

- **Healthcare:** In 2019, a US cybersecurity firm reported that an unnamed Indian healthcare website was hacked, with the hackers stealing the data of **68 lakh patients and doctors**. The stolen information included patient details, patient case history, doctor information, and other personal information.

- **Credit and debit cards:** In October 2019, a Singapore based cybersecurity firm reported that **13 lakh credit and debit card details** had been stolen, and were now on sale online. It ws reported that it was likely that this data stolen by placing a magentic stripe in an ATM that was able to copy the information of the user's card.

Is there privacy on Internet?

Privacy Policies of Telecom Service Providers

Airtel

- Explicitly states that provision of services is contingent upon consent to process data; may contravene PDPB
- No additional safeguards for sensitive personal data
- Reserves right to process personal data post termination of contract
- Data retention timelines and anonymisation standards not visible
- Unclear whether DND SMS stops messages or stops data collection and sharing
- Does not take consent before sharing data with third parties; may allow them to have lower security standards than itself

Sign language interpretation upon request.

Jio

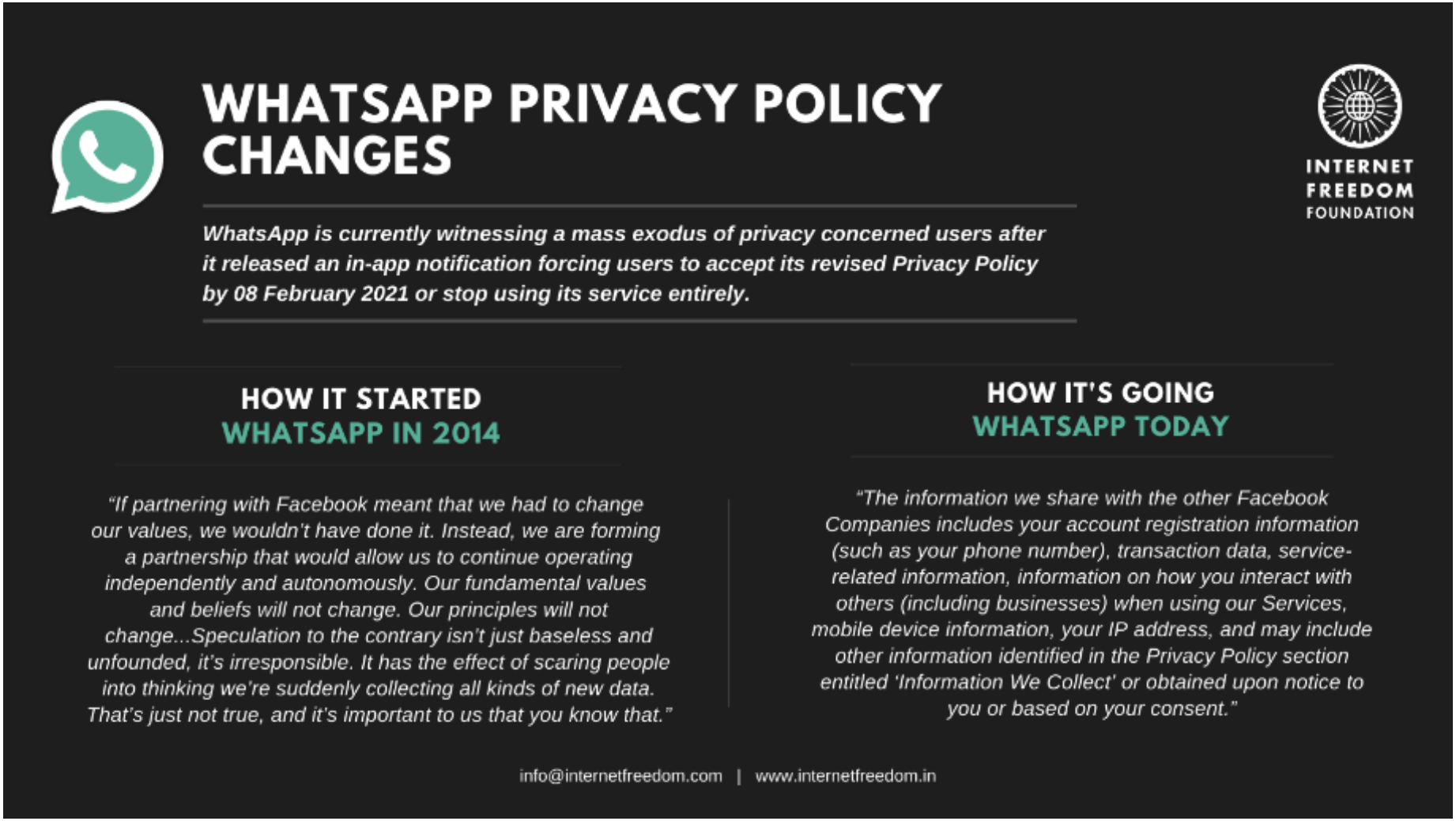
- Notes that Jio, "may not be able to process your request of correction, updation or deletion, in case... it is extremely difficult to implement". PDPB may not allow for such exemptions.
- Withdrawal of consent may lead to cancellation of services
- Again, data retention timelines and anonymisation standards not visible
- Also seems to hold its authorised third party partners to lower standards than itself.
- The policy lists 'hacking' as a case in which Reliance Jio exempts itself from responsibility in case of a breach of security. Now, the DoT's user license agreement also specifies that "The LICENSEE shall be completely and totally responsible for security of their networks."
- Lastly, the ambiguity over whether the DND SMS stops the collection and sharing of data persists here as well.

Sign language interpretation upon request.

Vi

- Seems to view the usage of services as equivalent to the provision of consent for the processing of data. May contravene PDPB as consent may not be free or capable of being withdrawn.
- Does not mention whether the withdrawal for processing certain data is viewed grounds for termination of services by Vi.
- Indicates that Vi may collect data about, "preferences for particular products, services or lifestyle activities".
- Inclusion of user in any telephone or similar directory following an opt-out model
- Sharing of anonymised information with authorised third parties also follows opt-out model
- Yet again, data retention timelines and data anonymisation standards are missing
- Also does not specify any consent sharing any mechanism for sharing data with authorised third parties.
- Ambiguity of the implications of the DND SMS remains here as well
- Vi's policy too seems to imply that it may allow the security standards of the third parties to be lax.

Sign language interpretation upon request.



Data Privacy In India

The Indian Privacy Code, 2018 builds off on an incremental process. It takes its foundation and inspiration from the Privacy (Protection) Bill, 2013 which was drafted over a series of roundtables and inputs conducted by the Centre for Internet and Society, Bangalore.

To update and to make it's scope comprehensive it has been drafted by distilling 7 privacy principles from various constitutional and expert texts..

7 Principles

- INDIVIDUAL RIGHTS ARE AT THE CENTER OF PRIVACY AND DATA PROTECTION
- A DATA PROTECTION LAW MUST BE BASED ON PRIVACY PRINCIPLES
- A STRONG PRIVACY COMMISSION MUST BE CREATED TO ENFORCE THE PRIVACY PRINCIPLES
- THE GOVERNMENT SHOULD RESPECT USER PRIVACY
- A COMPLETE PRIVACY CODE COMES WITH SURVEILLANCE REFORM
- THE RIGHT TO INFORMATION NEEDS TO BE STRENGTHENED AND PROTECTED
- INTERNATIONAL PROTECTIONS AND HARMONISATION TO PROTECT THE OPEN INTERNET MUST BE INCORPORATED

Campus Address :

88, Sector 44,
Gurgaon – 122002

CONTACT US

www.grm.institute

Email :
admissions@grm.institute

Thank you!