



Information Security  
Education & Awareness  
Project Phase – II  
**Privacy in the cyber space and  
cyber law**

By

**Prof(Dr.)Debarati Halder,**

LL.B, LLM(International & constitutional Law), LLM(Criminal  
& Security Law), Ph.D(NLSIU, Bangalore)

Professor of Law,

Parul Institute of Law, Parul University, Gujarat

Founder, Center for Cyber Victim Counselling

Founding Secretary, South Asian Society of Criminology &  
Victimology

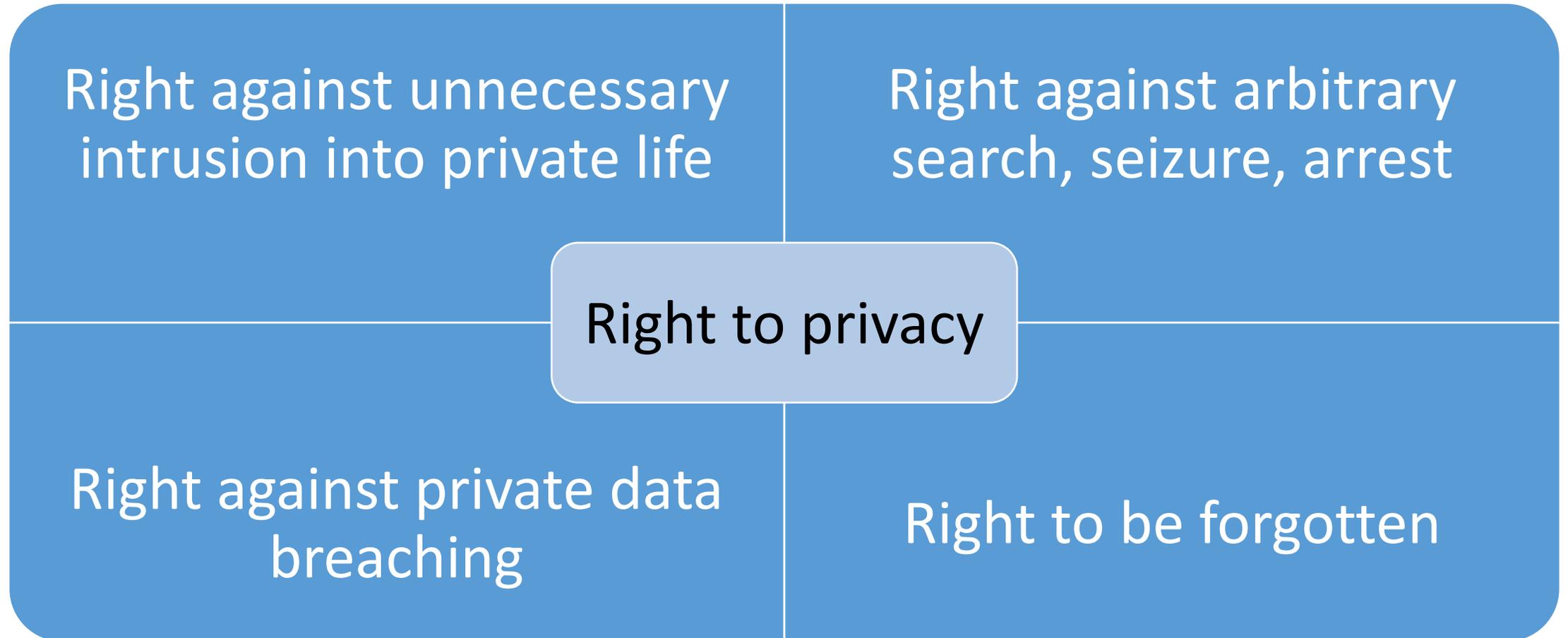
Trustee board member, International Society of Therapeutic  
Jurisprudence

# Conceptualising privacy



- No one should disturb when one wants privacy.
- No one should be allowed to enter the premises /room/snoop into digital devices without any solid reason.
- No one should be unnecessarily questioned about the work/activity done when in private mode

# Privacy : a myth or a reality



# Sensitive personal data : the reality

- S.3(35) Information Technology Act, 2000 (amended in 2008) & The Information Technology Reasonable security practices and procedures and sensitive personal data or information Rules, 2011 :
- “Sensitive Personal Data” means ***personal data revealing, related to, or constituting, as may be applicable—***
- (i) passwords;
- (ii) financial data;
- (iii) health data;
- (iv) official identifier;
- (v) sex life;
- (vi) sexual orientation;
- (vii) biometric data;
- (viii) genetic data;
- (ix) transgender status;
- (x) intersex status;
- (xi) caste or tribe;

# Who are the data generators? Processors? Data storing bodies ? Who knows our personal sensitive data?



# Consequences of privacy breach on cyber space

Unauthorised access to valuable information, monetary loss, threat to physical integrity

Ransom attack, sextortion, extortion

Impersonation

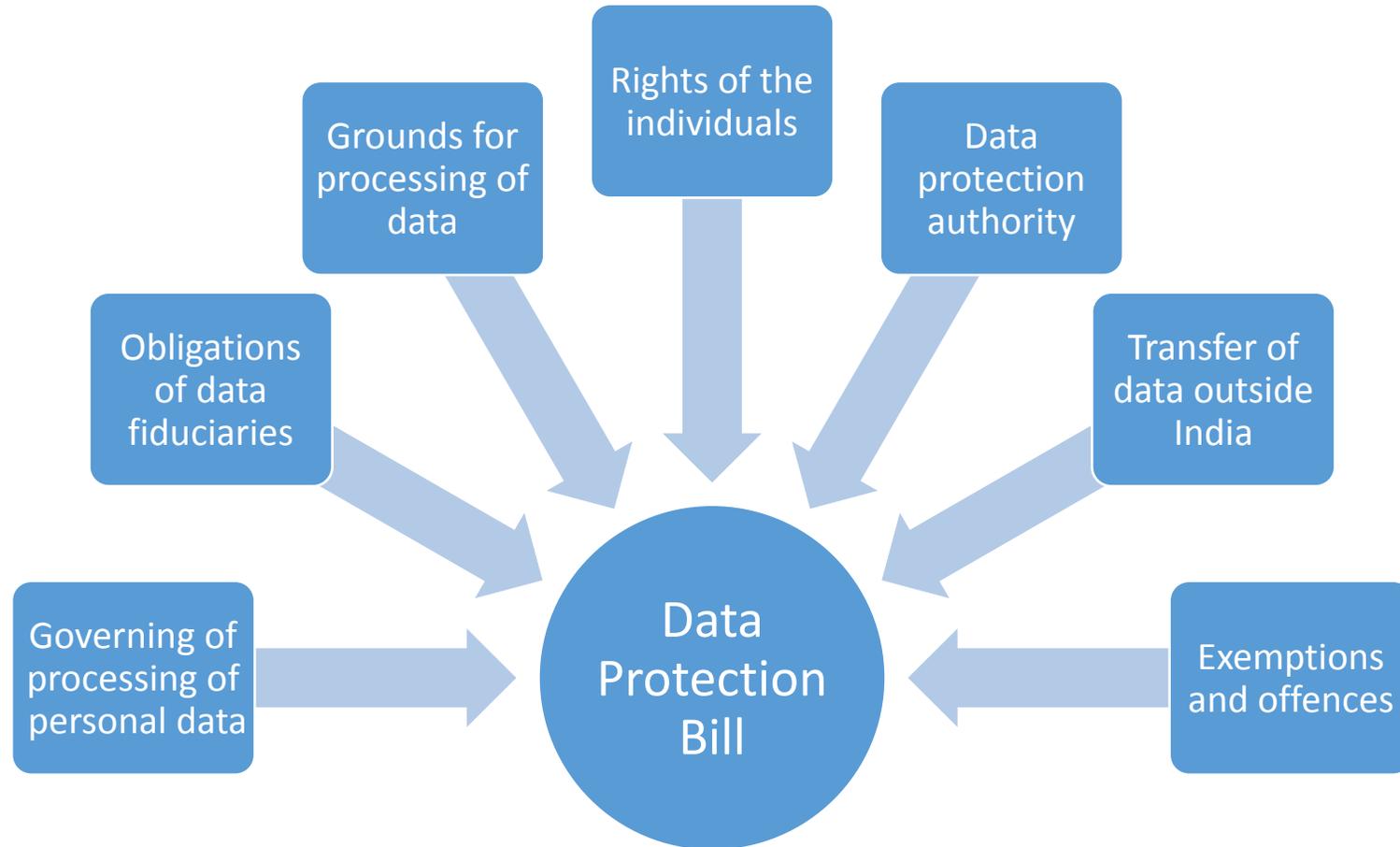
Revenge pornography

voyeurism

# Data Protection Bill, 2019 : an over view

- Introduced by : the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019 in Lok Sabha .
- Aim and objective of the Bill :
  - to provide for protection of personal data of individuals,
  - establish a Data Protection Authority for the same.
- Status: Not yet passed as a fullfledged law

# Significant points to remember for Data Protection Bill



# Do we have legal rights to protect our privacy

- Physical privacy flowing from UN Convention of Human Rights
- Art 21 of the Constitution of India
- Indian Penal Code
- Information Technology Act, 2000(amended in 2008) & some of its Rules
- Juvenile Justice Care and protection of Children Amendment Act, 2015
- Protection of Children from sexual offences Act
- Data Protection Bill, 2018
- European Union General Data Protection Regulations
- Domestic data protection related laws in different countries
- 4<sup>th</sup> Amendment to the constitution of the US providing rights against unreasonable search, seizure etc.

# Can our data be protected ?

- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. (S.43A IT Act, 2000, amended in 2008)
- Disclosure of information breaching a lawful contract even by intermediary (S.72A)
- Exceptions to S.79, IT Act : Due Diligence not applied

# How privacy is breached on cyber space



# How would one understand that data has been breached

- Suspicious mail /message /contents
- Change of profile contents
- Impersonating profiles/mails reaching out to contacts
- Outflow of banking data/ money
- Receiving calls from suspicious persons

# How to save phone, data and contents

- Filing complaint to the nearest police station
- Reaching out to SP /Judicial magistrate
- Two step verification system
- WhatsApp admin liability
- Cautious and judicious use of cloud storage
- Controlling self generated data

# Best practices vs worst practices

- Protect the evidence
  - Contact the website/company hosting personal data
  - Contact the police on an urgent basis
  - Reboot the devices
  - Refresh all passwords/user ids.
- Do not contact hackers
  - Do not reach out to senders of suspicious mails/messages
  - Do not destroy the evidences
  - Do not go ahead with old passwords, user ids.

Thank you

Prof(Dr)Debarati Halder

Professor of Law, Parul Univeristy &

Managing Director (Hon)

Centre for Cyber Victim Counselling

[www.cybervictims.org](http://www.cybervictims.org)

[profdebarati@gmail.com](mailto:profdebarati@gmail.com)

For more information on Cyber law please visit

**Gender and Internet : web magazine for cyber law for women**

@ <https://internetlegalstudies.com/>



[www.isea.gov.in](http://www.isea.gov.in)

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235