DATA PRIVACY AND SECURITY

Bharat Gupta

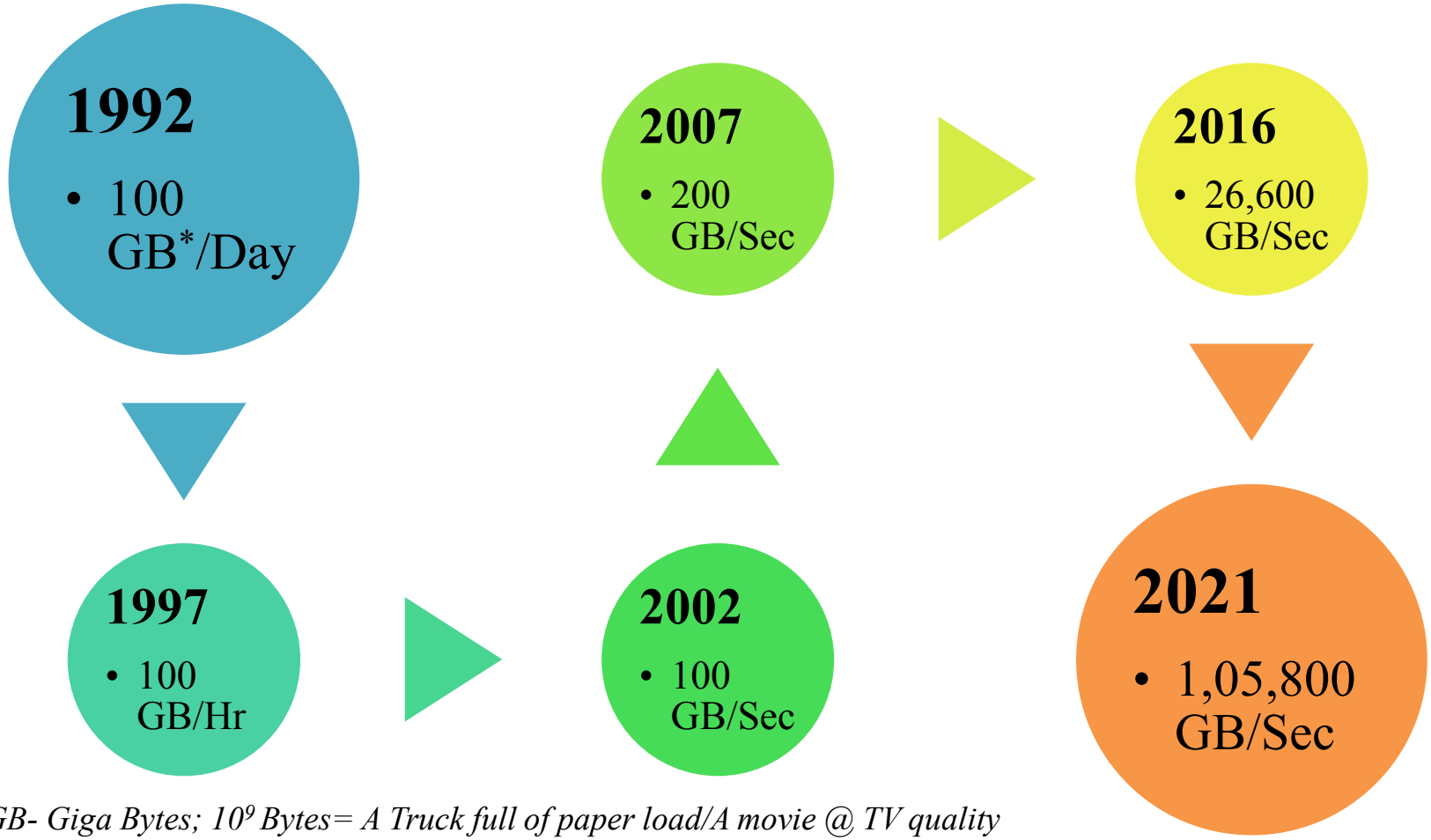
Telecom Regulatory Authority of India

Sequence

- Introduction.
- Digital Eco-System and Personal Data.
- Data Privacy Initiatives: World.
- Data Privacy Framework: India.
- Present Initiatives in India.

Introduction

DATA GROWTH



* *GB- Giga Bytes; 10^9 Bytes= A Truck full of paper load/A movie @ TV quality*

Source: Cisco VNI Global IP Traffic Forecast, 2016–2021.

ZETA(10^{21}) BYTE ERA

- **Annual global IP traffic will reach 3.3 ZB per year by 2021**, In 2016, the annual run rate for global IP traffic was1.2 ZB per year.
- **Global IP traffic will increase nearly threefold over the next 5 years :**Monthly IP traffic will reach 35 GB per capita by 2021, up from 13 GB per capita in 2016.
- **The number of devices connected to IP networks will be more than three times the global population by 2021(27.1 Billion Devices).**
- **Smartphone traffic will exceed PC traffic.** In 2016, PCs accounted for 46 % of total IP traffic, but by 2021 PCs will account for only 25 % of traffic. Smartphones will account for 33 % of total IP traffic in 2021, up from 13 % in 2016.
- **PC**-originated traffic will grow @ CAGR of **10 %**, **TVs @ 21%, tablets @29%, smartphones @ 49% and Machine-to- Machine (M2M) modules@ 49%.**
- **Traffic from wireless and mobile devices will account for more than 63 % of total IP traffic by 2021.**
- It would take more than **5 million years** to watch the amount of **video** that will cross global IP networks **each month** in **2021**.

Data is the new Oil!!

"From Hitler to Saddam, **Oil** has often been a dangerous Temptation"

DATA BREACH NEWS, ARTICLES AND UPDATES

Story behind how low-level Apple employee leaked iBoot source code

BY ROBERT ABEL FEBRUARY 14, 2018

The story behind the Apple iOS 9 source code leak played out much like a horror movie in which a close nit group of friends steal something for a good time only to open Pandora's Box.

Equifax data breach may have exposed a wider range of data

BY DOUG OLENICK FEBRUARY 09, 2018

Adversary breaches Tennessee hospital's medical records server to install cryptominer

BY BRADLEY BARTH FEBRUARY 09, 2018

Decatur County General Hospital in Parsons, Tenn., has publicly disclosed that an unauthorized party accessed the server for its electronic medical record system and secretly implanted cryptomining malware.

Waldo County, Maine, phishing attack results in data breach

BY ROBERT ABEL FEBRUARY 08, 2018

A phishing attack compromised the information of Waldo County employees in Maine.

Dial 'B' for Breach: Unauthorized party access data on 800K Swisscom customers

BY BRADLEY BARTH FEBRUARY 08, 2018

Telecom giant Swisscom yesterday disclosed that an unauthorized intruder misappropriated an unnamed sales partner's access to its data, thereby compromising basic information pertaining to approximately 800,000 customers.

Uber CISO to Congress: data breach extortion payment wasn't a true bug bounty

BY BRADLEY BARTH FEBRUARY 07, 2018

Testifying before members of Congress on Tuesday, Uber Technologies CISO John Flynn acknowledged that his company acted irresponsibly by waiting a full year before disclosing the breach of a third-party database containing information on 57 million customers and drivers.

Massachusetts attorney general adds online data breach report portal

BY DOUG OLENICK FEBRUARY 06, 2018

Massachusetts is trying to make it easier for businesses and organizations to report a data breach by setting up an online portal.

Phishing scam exposes W-2 forms of Keokuk, Iowa employees and officials

BY BRADLEY BARTH FEBRUARY 05, 2018

The small Iowan city of Keokuk has disclosed that a cybercriminal used a phishing scam to fraudulently obtain an electronic file containing the 2017 W-2 tax forms of current and former employees and elected officials.

DHS employee fumbled classified Super Bowl security documents

BY DOUG OLENICK FEBRUARY 05, 2018

A Department of Homeland Security staffer fumbled several classified documents in December creating a physical data breach.

Hacked cryptocurrency exchange to reimburse customers after largest heist in history

BY ROBERT ABEL JANUARY 29, 2018

Tokyo-based cryptocurrency exchange Coincheck Sunday told customers it would be repaying about 90 percent of the $534 million worth of NEM coin stolen.

South Dakota government advances data breach notification bill

BY DOUG OLENICK JANUARY 24, 2018

The South Dakota State Judiciary committee voted unanimously to advance a bill that would require companies to inform state residents if their PII was involved in a data breach.

Oh, baby! Infants' Social Security numbers spotted for sale on dark web

BY ROBERT ABEL JANUARY 23, 2018

The personal identifiable information (PII) of infants, including Social Security numbers, were spotted advertised for sale on the dark web.

Norwegian healthcare org fails GDPR breach notification standard

BY DOUG OLENICK JANUARY 22, 2018

The difficulty organizations may have complying with the EU's General Data Protection Regulation (GDPR) became apparent when a Norwegian health care group took too long to report a data breach earlier this month.

Aetna agrees to $17M to settle data breach

BY DOUG OLENICK JANUARY 19, 2018

Aetna will pay a $17.1 million as part of a settlement for a July 2017 data breach that may have compromised the information of thousands of HIV patients.

Separate ransomware attacks strike New Mexico city, Indiana health care provider

BY BRADLEY BARTH JANUARY 19, 2018

A New Mexican city of roughly 45,000 people and an Indianan hospital operator have fallen victim to separate ransomware attacks this month. In other localized news, a data breach at a third-party educational testing service exposed information belonging to 52 students in New York State.

Jason's Deli reports possible POS data breach

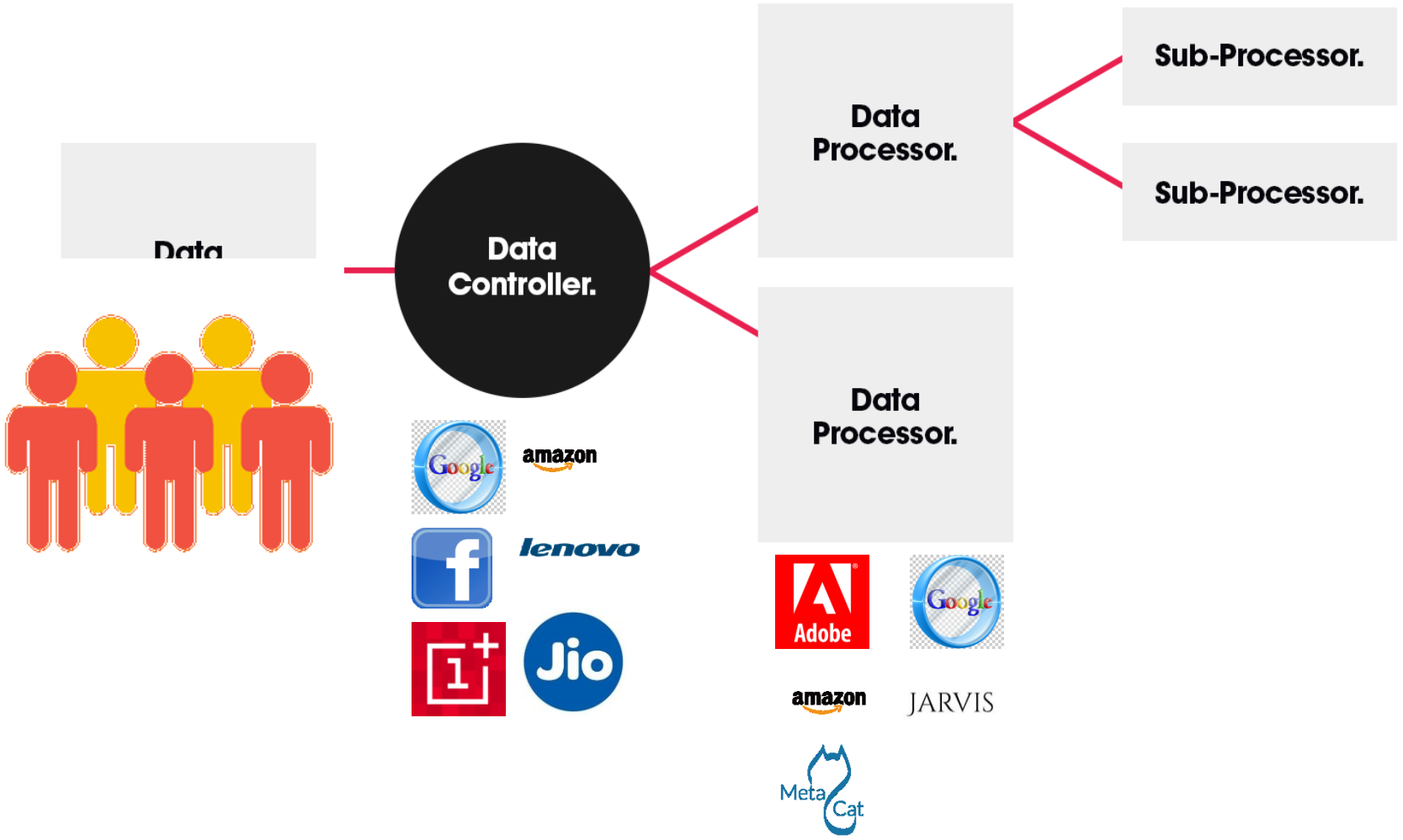
BY DOUG OLENICK JANUARY 10, 2018

The 266-location Jason's Deli is notifying its customers that their payment card information may have been compromised through a point of sale data breach.

Digital Eco-System & Personal Data

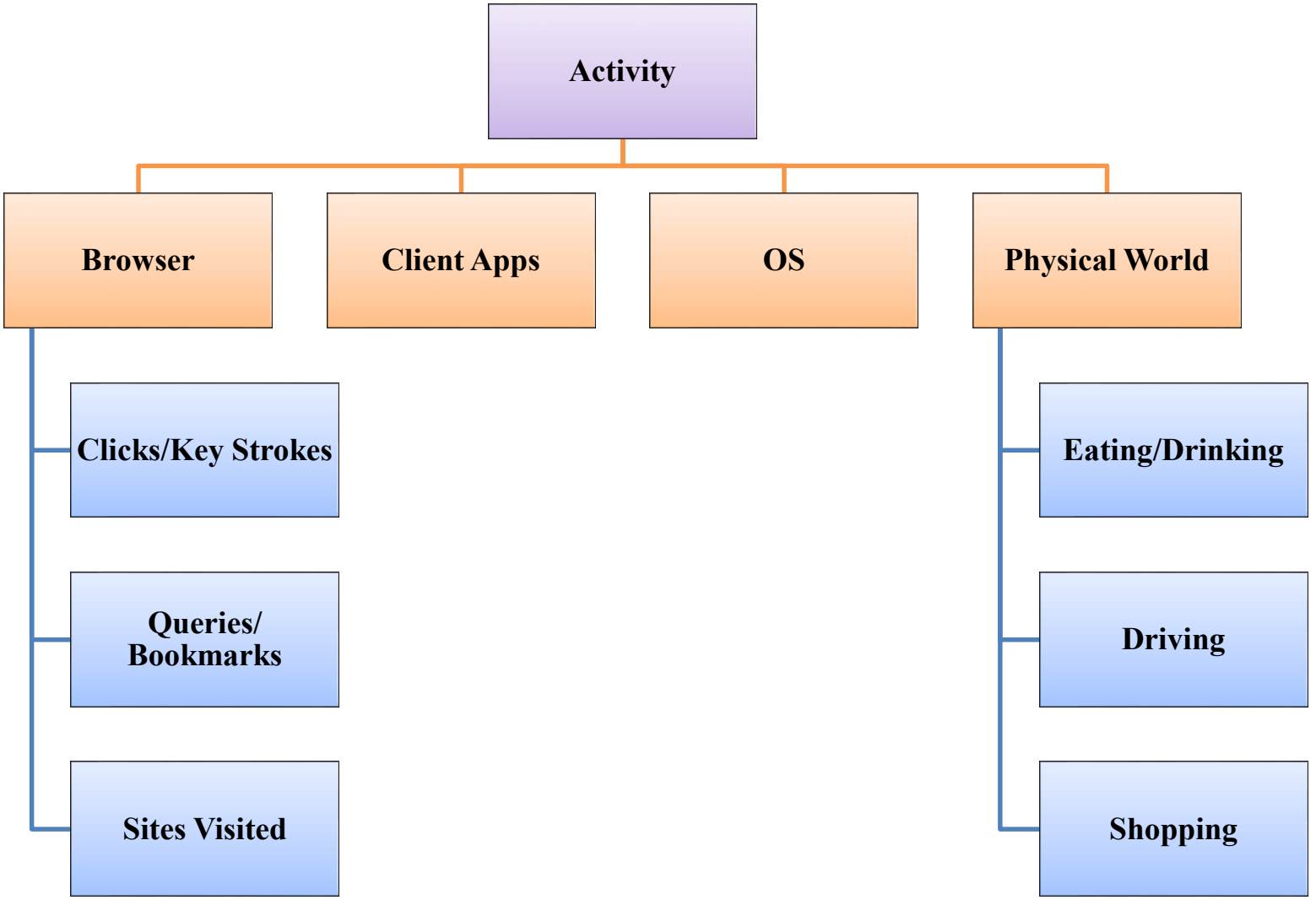
Digital Eco-System

Data Collection & Processing

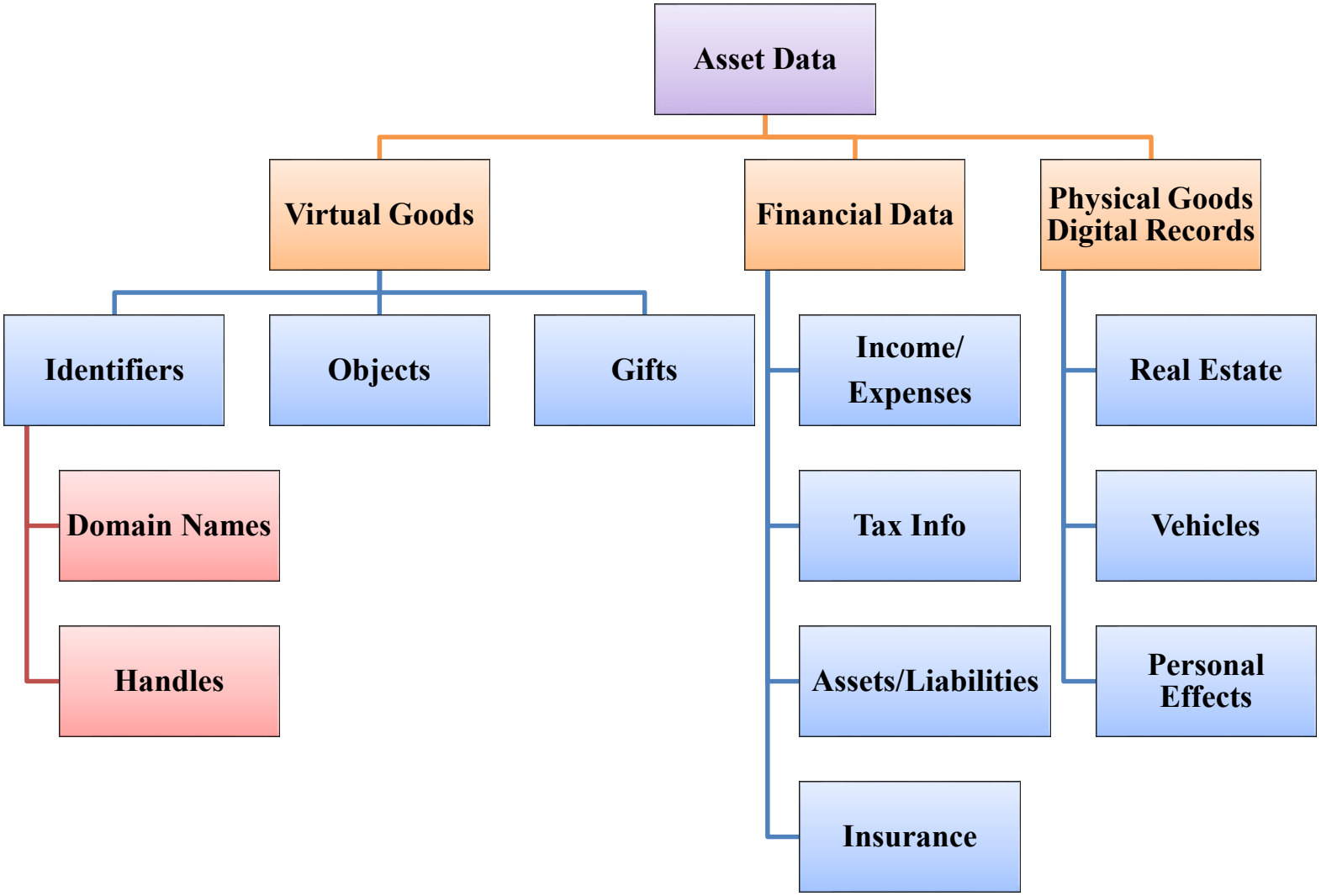


Personal Data Collection

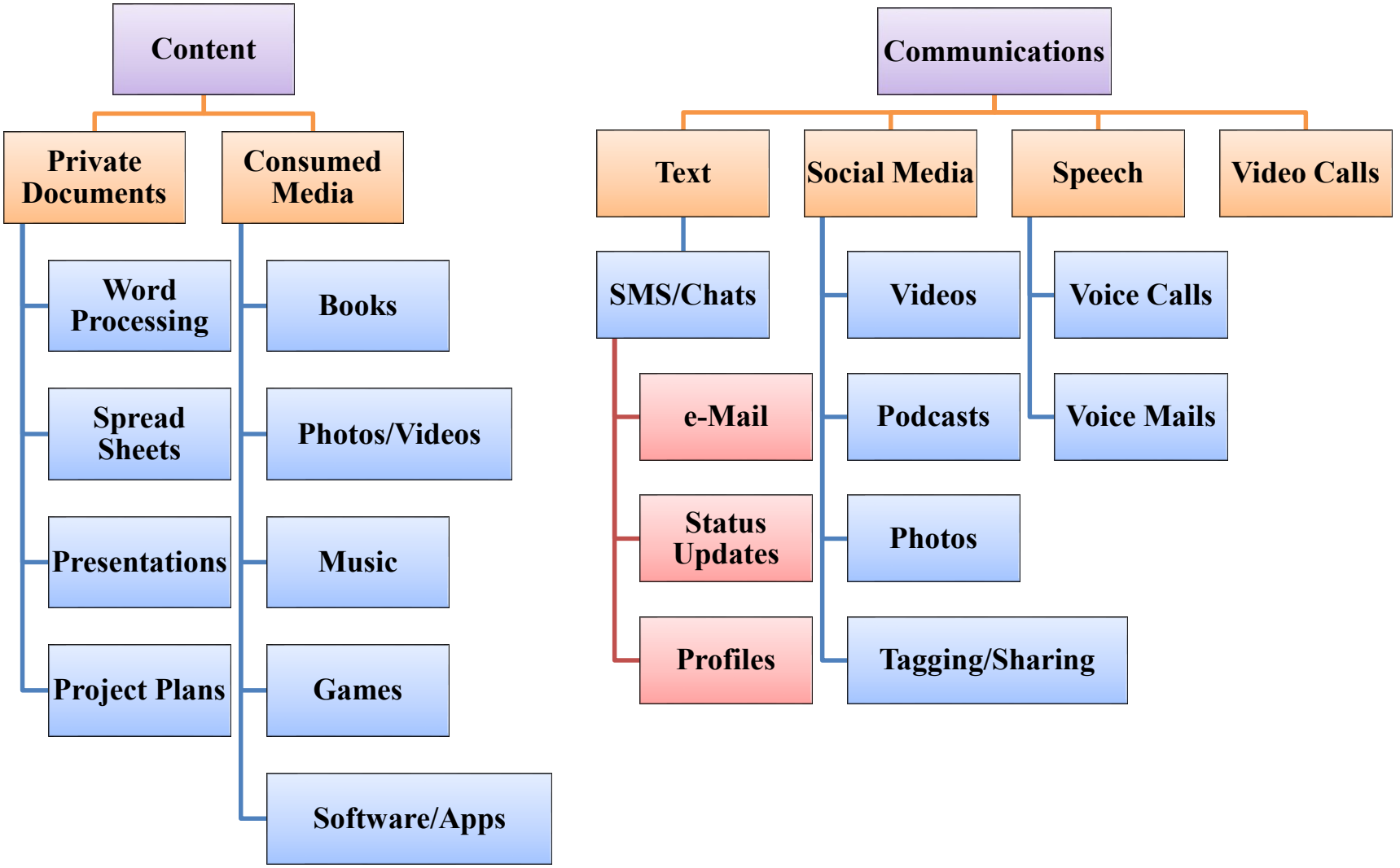
Personal Data Collection



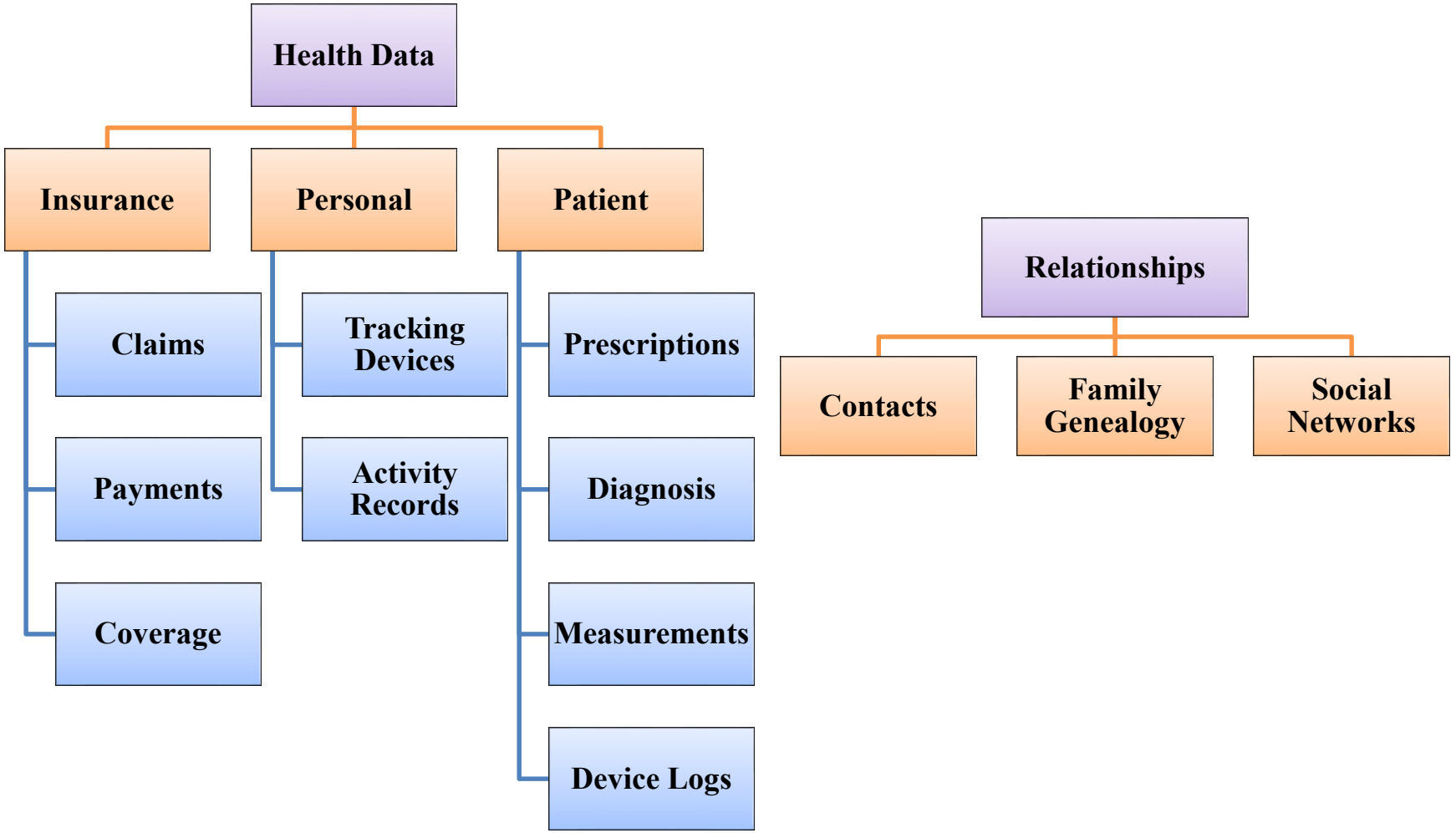
Personal Data Collection



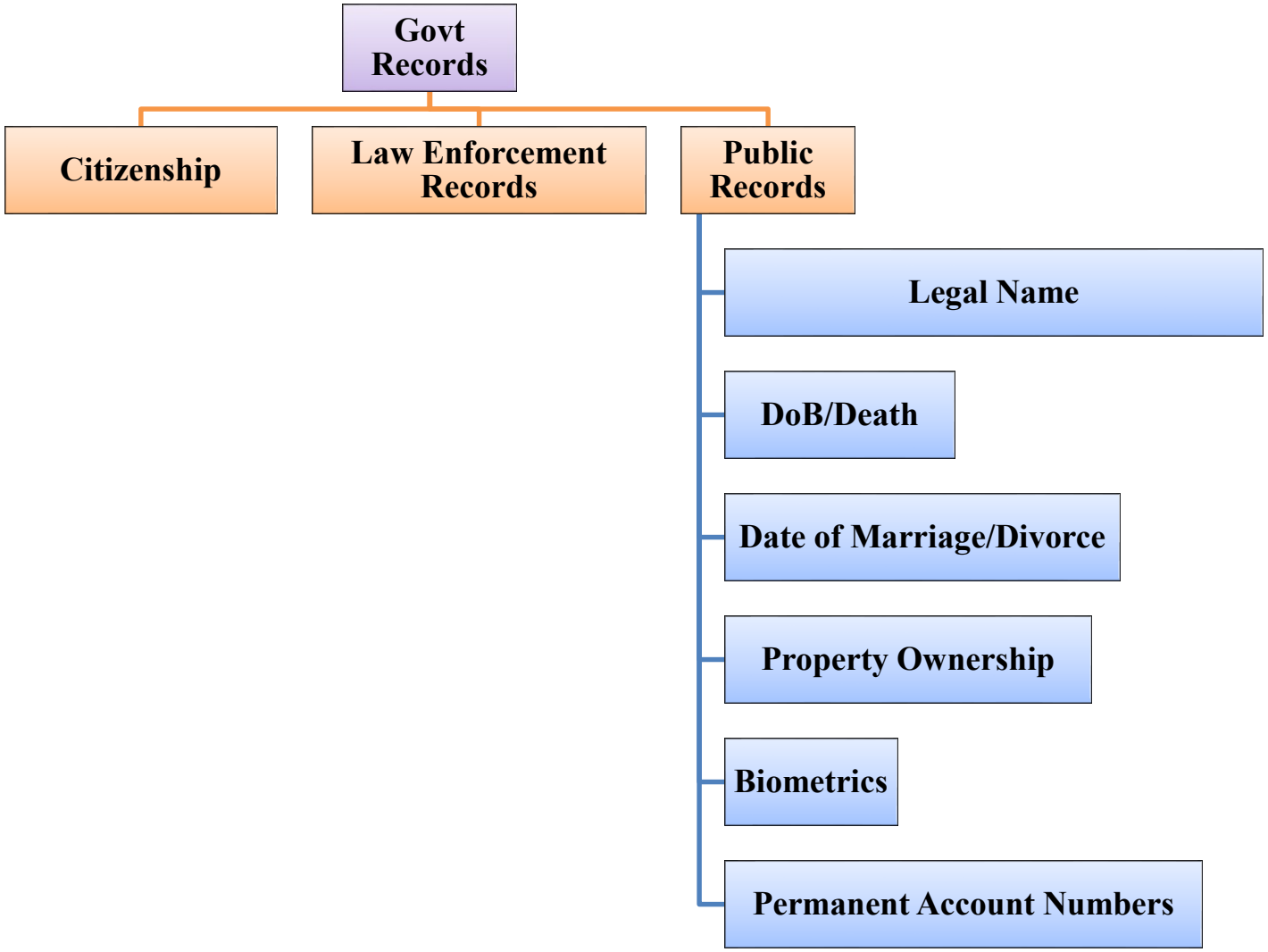
Personal Data Collection



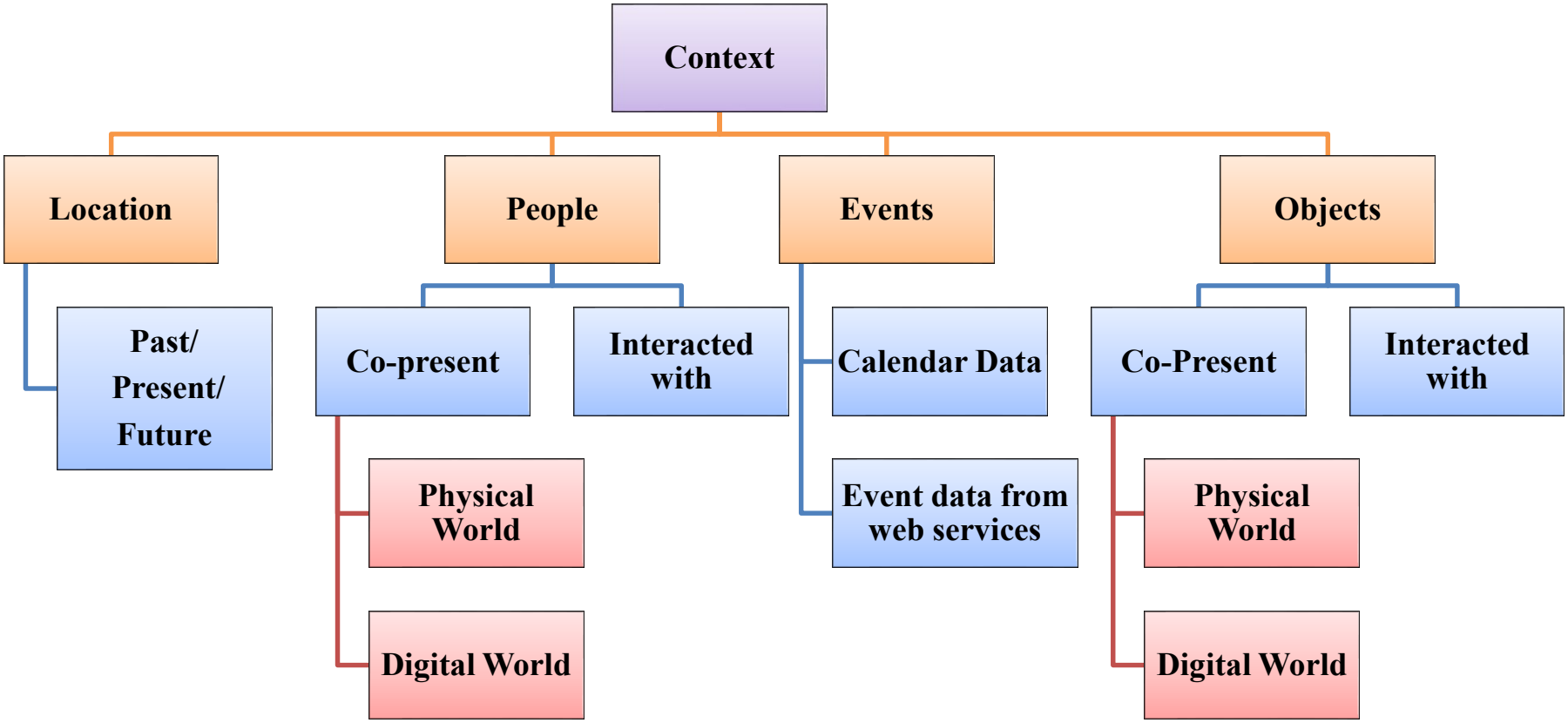
Personal Data Collection



Personal Data Collection



Personal Data Collection

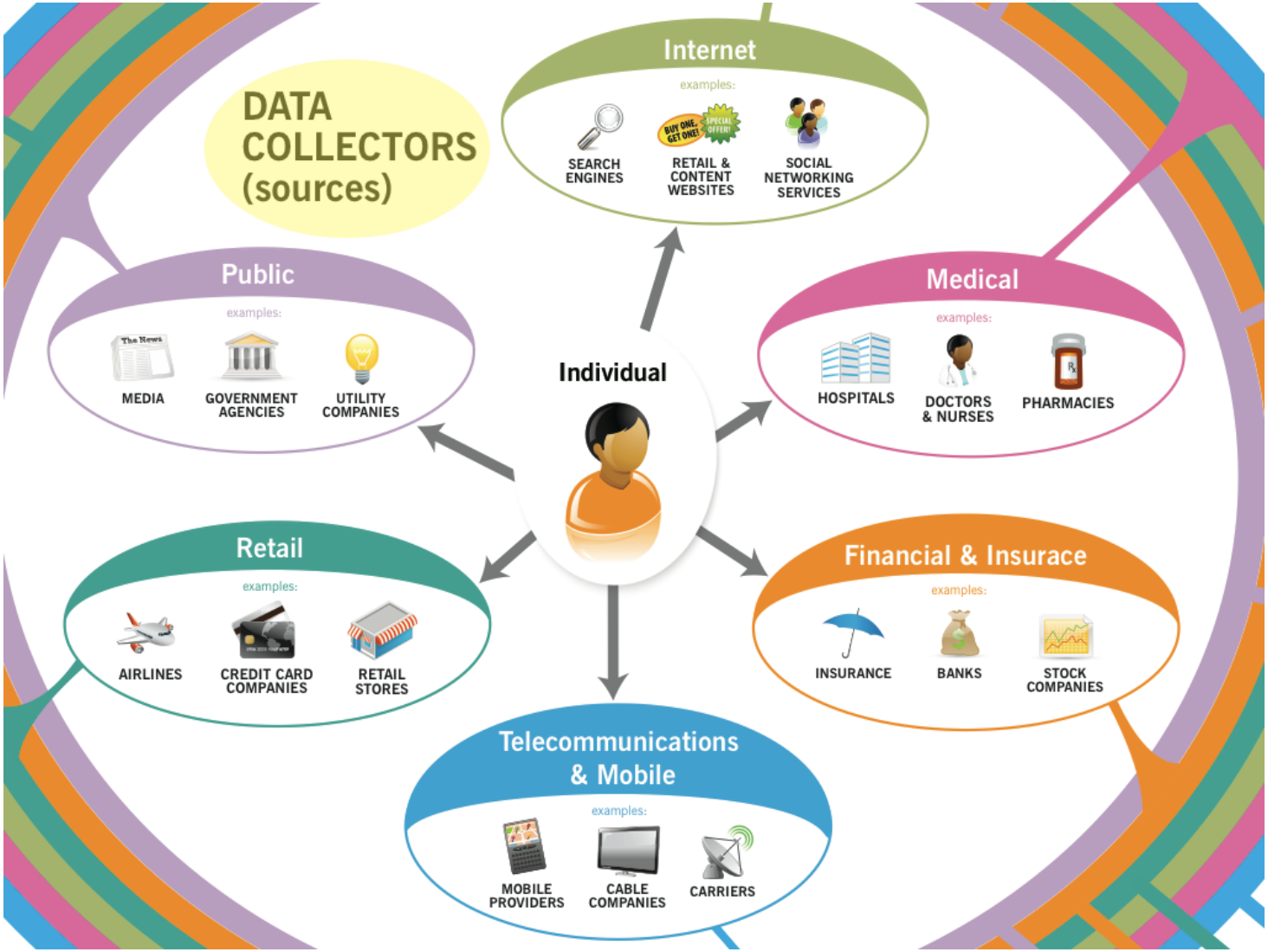


When You are Online, what happens in the background?

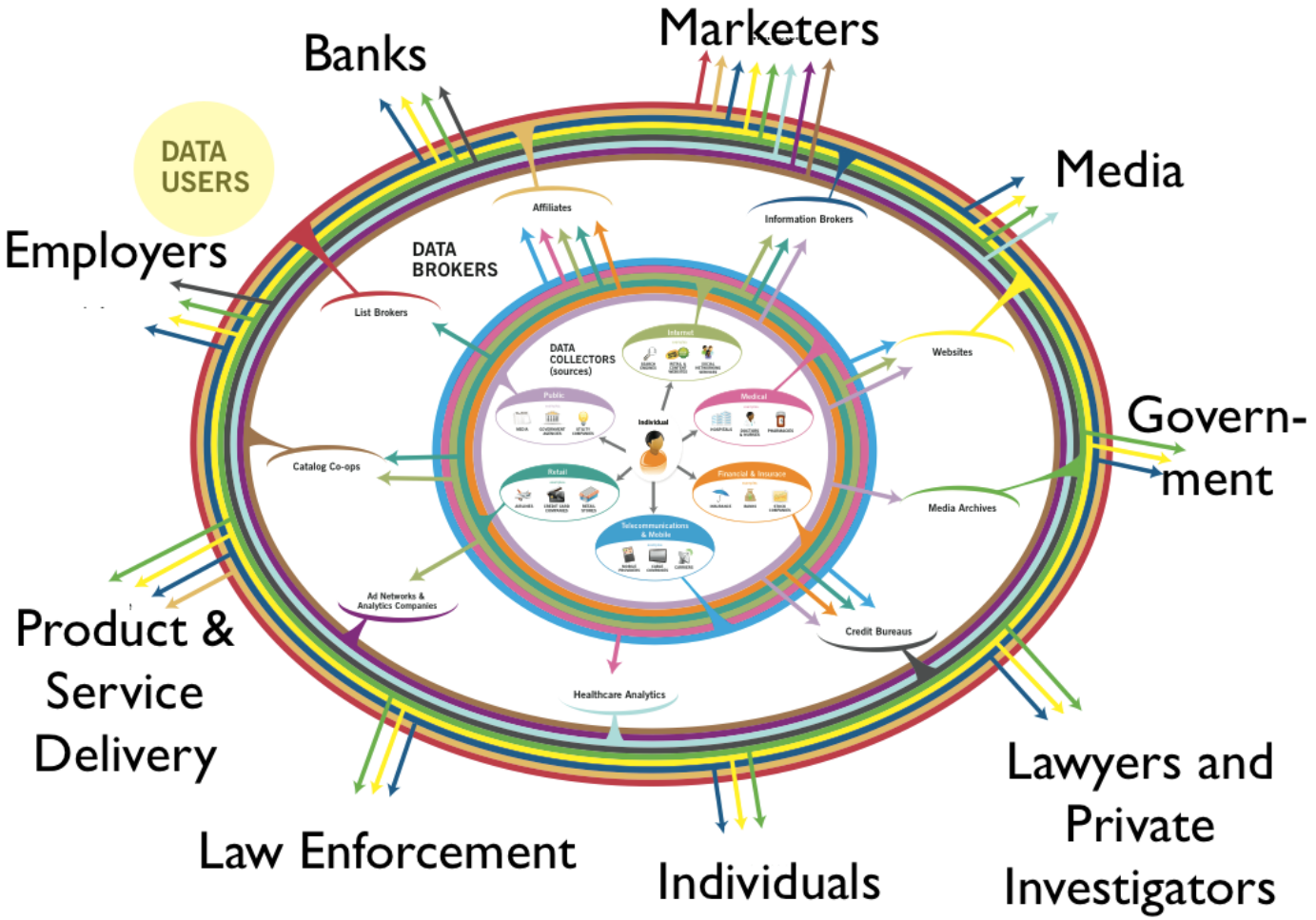
Your Profile and Identity is built

Types of data collected:
- Device id, location data, browser history, your OS,
- Anything else you may have given ‘permission’ to
access – eg, contact info, etc

What Happens to Personal Data?



What Happens to Personal Data?



Videos

Man commits suicide inside Northeast Express train

More Videos >

Business

Stay invested in MFs with sound track record

moneyTips

More Business stories >

#LifestyleTips

6 Sexy Valentine's Day Gifts for Her

More in Lifestyle Tips >

Cricket

Dravid's kind gesture wins hearts in India and Pakistan

cricketLives

More Cricket stories >

Movies

Is Hrithik convincing as mathematician Anand Kumar? Vote!

celebrityLives

More Movies stories >

News

At 97, yoga guru is India's oldest Padma Shri

healthTips

More News stories >

Valentine Flowers

Valentine Gifts - Be My Valentine

MRP Rs.1330

More like this >

Personal Care & Beauty Accessories

Gadget Hero's Snore Stopper Anti Snore Silicone Nose Clip For Sleep Apnea

MRP Rs.702 Rs.349 More like this >

Business

Soon you can taste the thunder overseas!

foodIndustry

More Business stories >

Cricket

Why Sanjay Manjrekar became a commentator

cricketReports

More Cricket stories >

Get Ahead

Our fearless future: 30 young Indians the world should know

Rings

Royal Jewellery Gold Plated Alloy Swarovski Zirconia

Movies

Sunny, Sushmita, Kajol: Who is the hottest?

Business

Divided over a river, TN, Karnataka to join hands for

Bags

Sling Bag for Men - Cosmus Stitchwell Cross Body Sling Bag -

MRP Rs.999 Rs.399

More like this >

Get Ahead

11.11, Eka, Maku: Meet India's new philosopher-entrepreneurs

fashion

More Get Ahead Stories >

News

India needs to tread softly on the Maldives

foreignAffairs

More News stories >

News

LIVE! After haemorrhaging for 4 days, Sensex recovers

More News stories >

News

Is defence hike enough to modernise armed forces?

defence

More News stories >

Kitchen Utilities (Misc)

2 X Refrigerator Fridge Multi-partition Storage Rack Fresh

MRP Rs.288

More like this >

Videos

Watch: Congress workers stage 'pakoda protest'

More Videos >

Get Ahead

Take the #PadMan challenge: Post your selfie!

bollywoodLives

More Get Ahead stories >

Cricket

Confident India aim to keep top spot as they take on injury-hit SA

cricketReports

More Cricket stories >

#GadgetTips

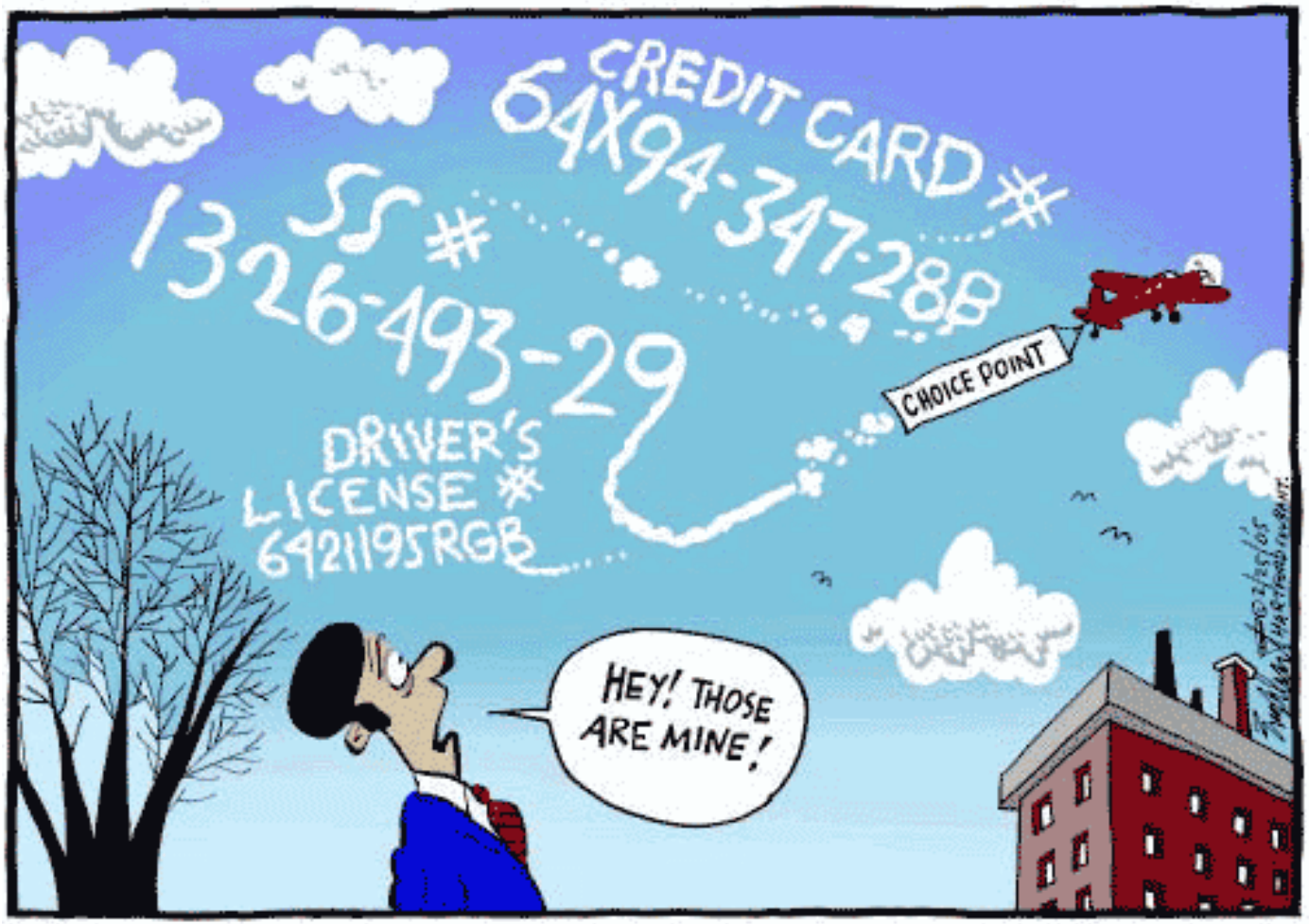
11 Gadgets That Will Make You Love Your Smartphone Even More

More in Gadget Tips >

hourly deal

Exclusive Heart Photo Pendant - Rs.149

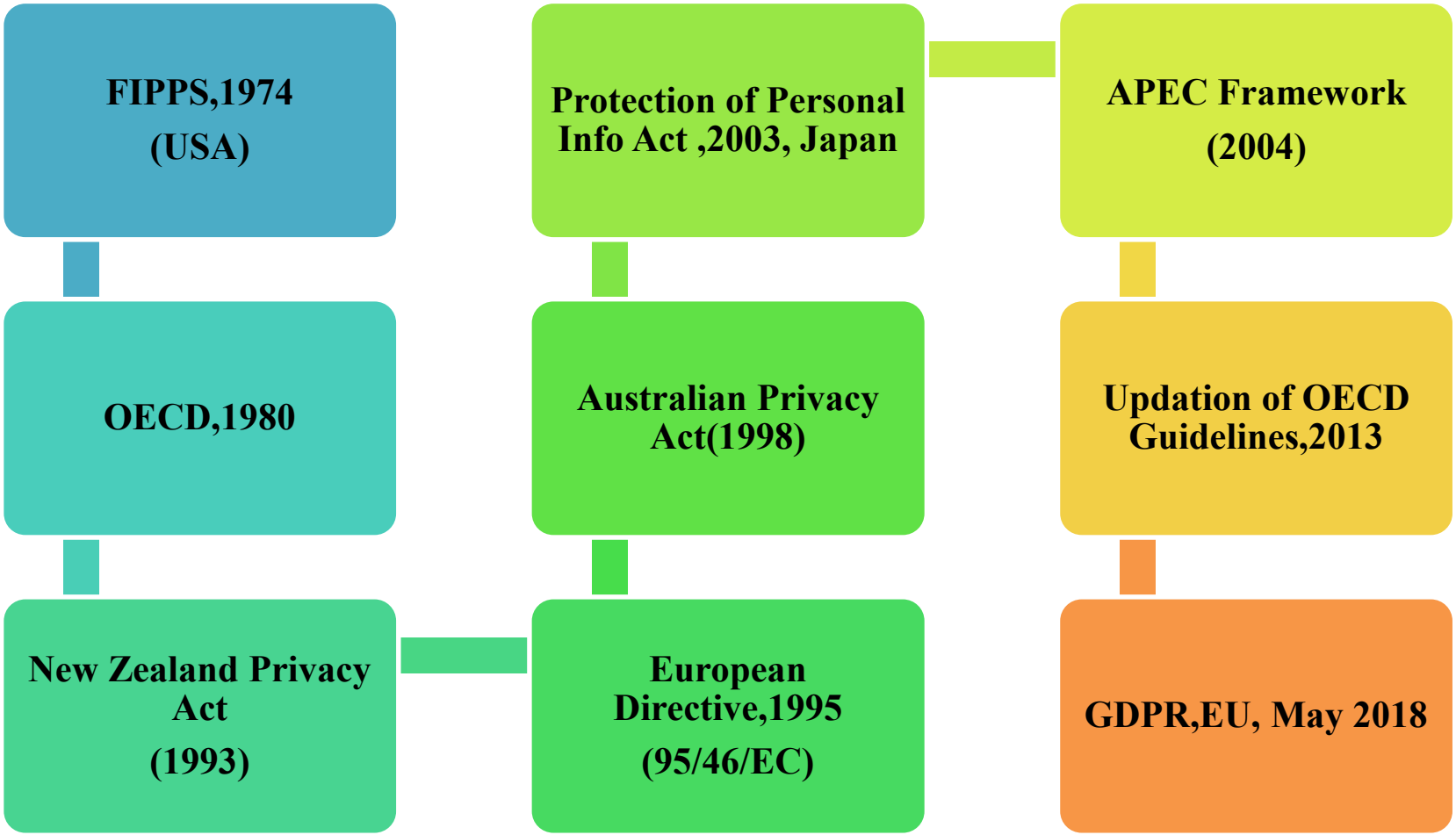
More like this >



Scary!! Are you protected?

Data Privacy Initiatives: World

DATA PRIVACY INITIATIVES : WORLD



DATA PRIVACY INITIATIVES: WORLD

- USA.
- APEC(Asia-Pacific Economic Cooperation).
- OECD(Org for Economic Cooperation and Development).
- EU (European Union).

DATA PRIVACY LAWS: USA

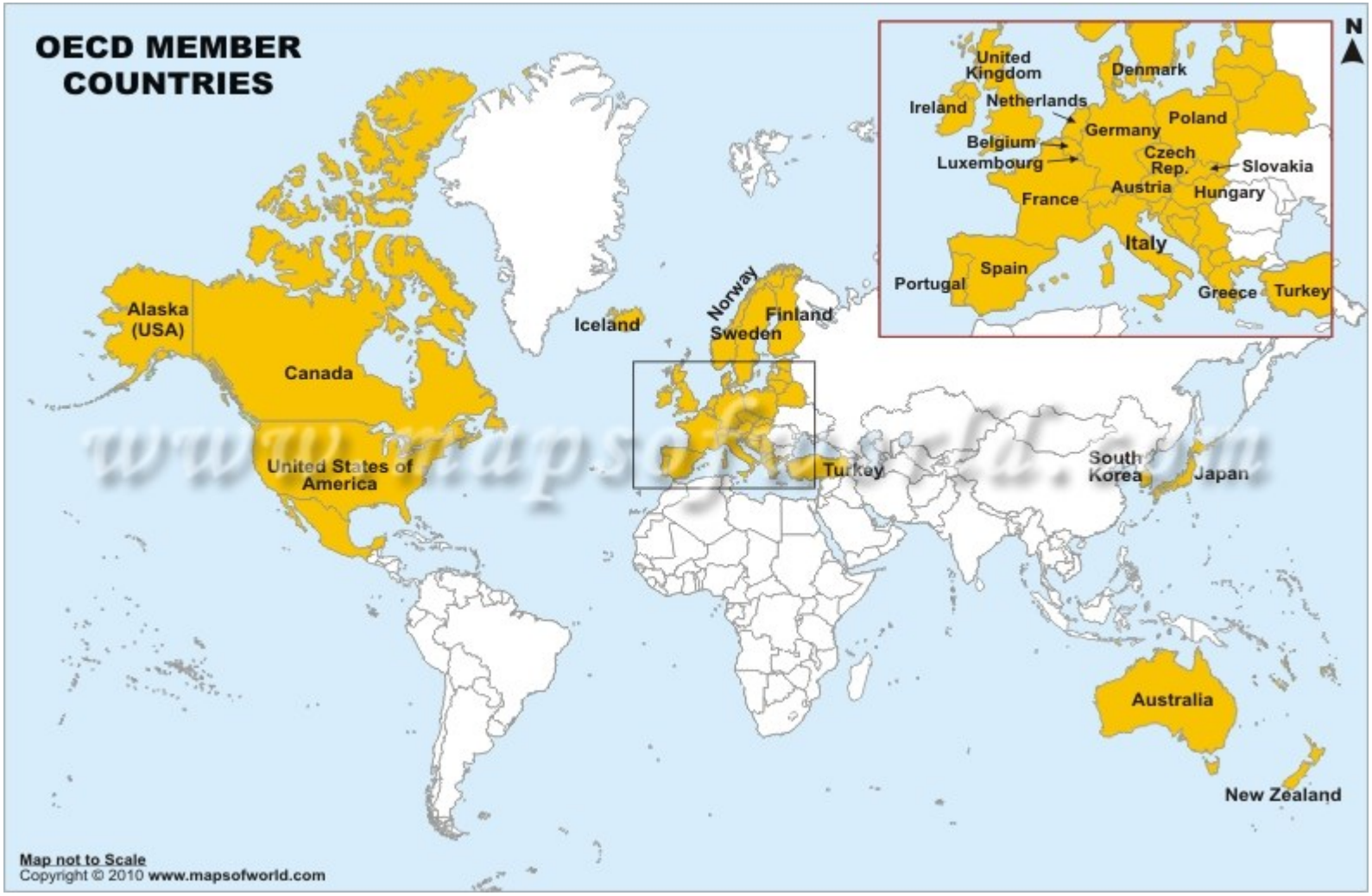
The United States has about 20 sector specific or medium-specific national privacy or data security laws, and hundreds of such laws among its 50 states and its territories. (California alone has more than 25 state privacy and data security laws). These laws, which address particular issues or industries, are too diverse to summarize fully in this volume.

In addition, the large range of companies regulated by the Federal Trade Commission ('FTC') are subject to enforcement if they engage in materially unfair or deceptive trade practices. The FTC has used this authority to pursue companies that fail to implement reasonable minimal data security measures, fail to live up to promises in privacy policies, or frustrate consumer choices about processing or disclosure of personal data.

DATA PRIVACY LAWS: USA

- US privacy protection is essentially a liberty protection. i.e protection of personal space from the Govt.
- US Constitution does not explicitly grant "Right to Privacy".
- US privacy laws hinges on the 1st,4th,5th and 14th Amendments to the US Constitution.
- Data Protection approach is different for Public and Pvt Sectors.
- Core data protection is based on Notice and Consent.
- Stringent Norms for Govt processing of personal info, while Notice and Choice based consent for Pvt Sector data processing.

PRIVACY GUIDELINES: OECD



PRIVACY GUIDELINES: OECD

- Initially Issued in 1980, revised in July 2013.
- Guidelines apply to personal data, whether in the public or private sectors.
- ***Eight*** Basic Principles of Application:
  1. **Collection Limitation**: limits to the collection of personal data.
  2. **Data Quality**: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
  3. **Purpose Specification**: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes specified on each occasion of change of purpose.
  4. **Use Limitation:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified.

PRIVACY GUIDELINES: OECD

- Basic Principles of Application……
  5. **Security Safeguard**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
  6. **Openness:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
  7. **Individual Participation:** Individual Rights are supreme and have to be regarded by the Data Controllers.
  8. **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

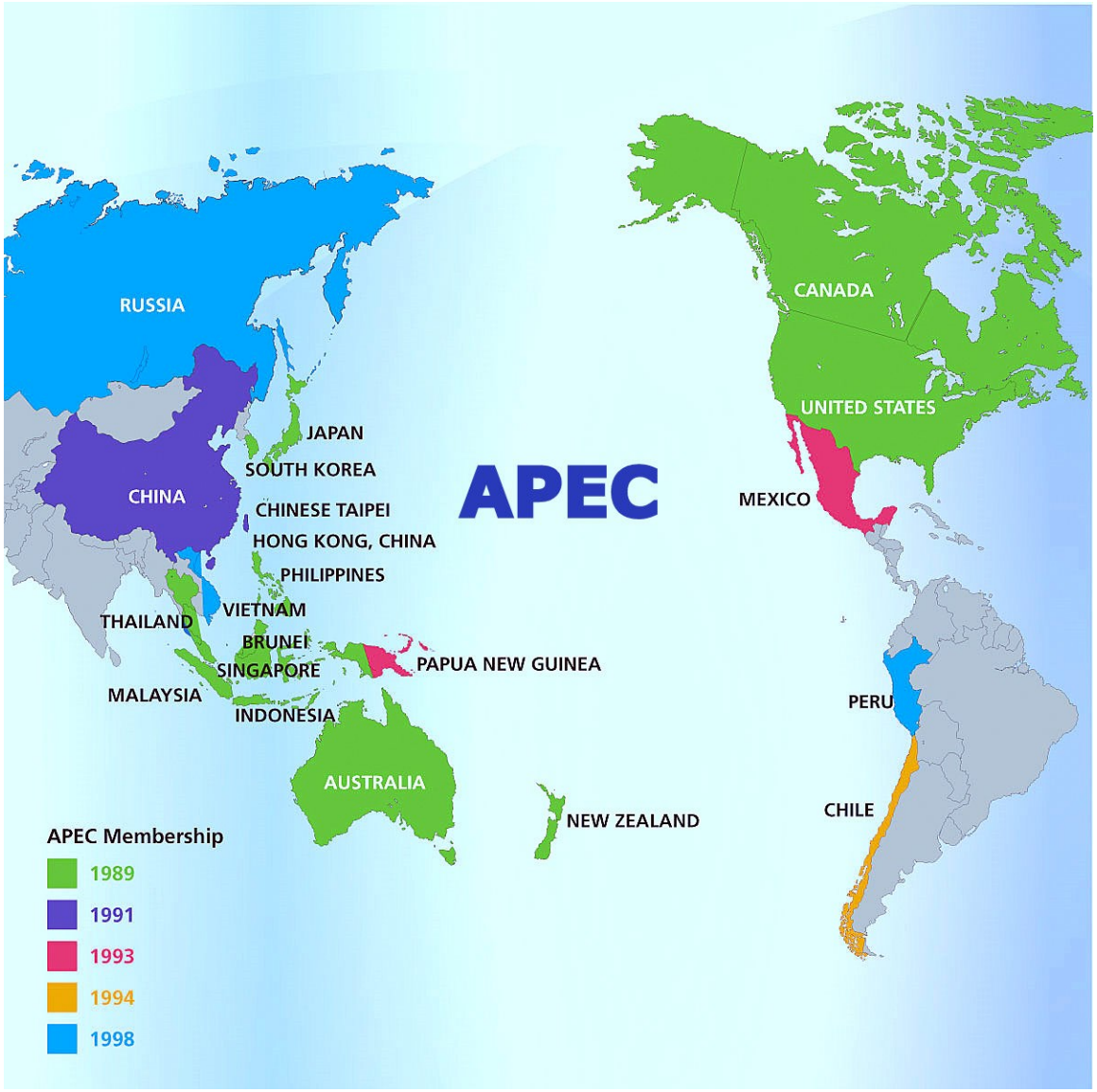
PRIVACY GUIDELINES: OECD

- Other Issues:
  - A data controller remains accountable for personal data under its control without regard to the location of the data.
  - A Member country should refrain from restricting trans-border flows of personal data between itself and another country where:

    (a) Other country substantially observes these Guidelines or

    (b) Sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.
  - Any restrictions to trans-border flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.
- Introduction of:
  - Privacy Management Programs to enhance accountability of Data Controllers.
  - Data Security Breach Notification.
  - Cross Border data flow and International co-operation.

DATA PRIVACY PRINCIPLES: APEC



APEC Information Privacy Principles

- Based on ***Nine*** Principles:
  1. Preventing Harm
  2. Notice
  3. Collection Limitations
  4. Uses of Personal Information
  5. Choice
  6. Integrity of Personal Information
  7. Security Safeguards
  8. Access and Correction
  9. Accountability

APEC information privacy principles

1. **Preventing harm**: Personal information protection should be designed to prevent he misuse of such information. Specific obligations/remedial measures should be proportional to likelihood and severity of the harm threatened by collection, use and transfer of personal information
2. **Notice**: Personal information controllers should provide clear statements while collecting personal information, purpose of the collection, who the information might be disclosed to, the identity and location of the controller, Available choices to limit the use and disclosure of the information and how to access and correct the information if needed, reasonably practicable steps to ensure notice is provided either before or during time of collection, or as soon after as is practicable.
3. **Collection limitation**: collection should be limited to relevant purposes and any such personal information should be obtained by lawful and fair means and , where appropriate, with notice to or consent of the individual concerned.

APEC information privacy principles

4. **Uses of personal information**: should be used only to fulfill the purposes of collection and other compatible or related purposes, unless get consent of the individual or for legal reasons.
5. **Choice**: where appropriate, individuals should be provided with clear, easily understandable, accessible, and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.
6. **Integrity of personal information**: should be accurate, complete and up-to-date to extent possible for the purposes of use.
7. **Security safeguards**: should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held and should be reviewed periodically

APEC information privacy principles

8. **Access and correction**: individuals should have access to their information, they should be able to challenge the accuracy of the information and, if possible as appropriate, have the information rectified, competed, amended or deleted.
9. **Accountability**: controller should be accountable for complying with Principles and should, if transferring the information, either get consent of the individual or take reasonable steps to ensure recipient will follow the Principles.

- Issues related to Cross Border Data Flow:
  - **CBPR**(Cross Border Privacy Rules, 2011): Encourage Free flow of data between member countries. Each member country to establish a Privacy Enforcement Authority(PEA) for implementing CBPR.
  - **CPEA**(Cross-border Privacy Enforcement Agency): CPEA is a multilateral mechanism which enables PEAs in the APEC region to cooperate in cross-border privacy enforcement of Privacy Laws.

EUROPEAN UNION

EUROPEAN UNION: GDPR

- GDPR(General Data Protection Regulation).
- Will be effective from **25 May 2018**.
- While US Rules emphasized on "***Liberty***" the EU Regulations are skewed towards " ***User Rights***".
- The regulation is intended to establish ***one single set of data protection rules across Europe***.
- Organizations outside the EU are subject to this regulation when they collect data concerning any EU citizen.
- Designed to give individuals better control over their personal data held by organizations, Each organization to appoint a ***Data Protection Officer***.
- Personal data is defined as "*Any information relating to a person who can be identified directly or indirectly. This includes online identifiers, such as IP addresses and cookies, if they are capable of being linked back to the data subject*".

EUROPEAN UNION: GDPR

- ***Indirect information*** might include "***physical, physiological, genetic, mental, economic, cultural or social identities that can be linked back to a specific individual***".
- There is no distinction between personal data about an individual in their private, public or work roles – all are covered by this regulation.
- Substantial increase in fines for organizations who do not comply:
  - ❖ Penalties can be levied up to the greater of ten million Euros or two per cent of global gross turnover for violations of record-keeping, security, breach notification and privacy impact assessment obligations.
  - ❖ These penalties are doubled to twenty million Euros or four per cent of turnover for violations related to legal justification for processing, lack of consent, data subject rights and cross-border data transfers.

EUROPEAN UNION: GDPR

- Data protection safeguards must be designed into ***products*** and ***services*** from the earliest stages of development.
- Compulsory pseudonymisation and/or encryption of personal data.
- Companies must report breaches of security by notifying the appropriate supervisory authority ***with in 72 hours*** after having become aware of it.
- Stringent Consent Mechanisms.
- Data Obtained must be for specific, Explicit and Legitimate Purpose.
- Explicit declaration of period for which data would be held by the data controllers.
- Some of the Important user rights under GDPR:
  - Right to Access, Edit and Erase data.
  - Right to Withdraw Consent.
  - Right to be Forgotten.
  - Right to know the purpose of data acquisition.
  - Right to Lodge Complaints.

EUROPEAN UNION: GDPR

- For Cross-border data transfer, three mechanisms have been created:
  - **Adequacy Test**(*Article 45*): Personal data of EU citizens to non-EU Areas is not permitted unless those countries are deemed to have an "Adequate" level of data protection. The decision in r/o of Adequacy would be taken by European Commission.
  - **Model Contractual Clause**: The European Commission has the power to decide that certain standard contractual clauses offer sufficient safeguards with respect to data protection while undertaking transfer of data to non-EU countries. The Commission has issued two sets of standard contractual clauses: one for transfers from data controllers to data controllers established outside the EU; and one set for the transfer to processors established outside the EU.
  - **Binding Corporate Rules** (*BCR*): These are internal rules (such as codes of conduct) which are adopted by a MNC. BCRs define the global policy of MNC with regard to the international transfers of personal data within the same corporate group, to entities located in countries, which do not provide an adequate level of protection.

Data Privacy Framework: India

Data Privacy Framework: India

- IT Act 2000
- Amendment to IT Act, 2008
- SPDI Rules, 2011
- Aadhar Act,2016
- Credit Information Companies(Regulation) Act,2005 and 2006.
- RBI Circulars.
- Indian Telegraph Act,1885.
- Indian Wireless Telegraphy Act,1933
- TRAI Act,1997
- Clinical Establishment Rules,2012.
- Indian Medical Council Act,1956
- Justice A P Shah Committee Report,2012

Present Initiatives

- TRAI: Consultation Paper on “Privacy, Security & Ownership of Data in Telecom Sector issued on 09 Aug 2017.
- On 24 Aug 2017, A nine-judge bench of the Supreme Court had ruled that Indians enjoy a fundamental right to privacy, that it is intrinsic to life and liberty and thus comes under Article 21 of the Indian constitution.
- On 27 Nov 2017, Govt of India had constituted a Committee of Experts under the Chairmanship of former Supreme Court Justice Shri B N Srikrishna to study various issues relating to data protection in India and make specific suggestions on principles to be considered for data protection in India and suggest a draft Data Protection Bill.

White Paper of the Committee of Experts on Data Protection Framework for India

Overview

- White Paper issued on 27 Nov 2017.
- The white paper is divided into **five** parts (233 Pages).
- Within each part, there are numerous chapters dealing with separate issues.
- Each chapter broadly follows a similar structure:
  a) The issue is set out.
  b) Account of comparative practice from other nations (primarily the EU, Europe, Canada, Australia, and South Africa).
  c) Committee's tentative view is set out.
  d) There are a series of specific questions for responding.

Overview

Part-1

- **Context Setting**(Pg 1-23): Gives a historical background of the paper including some broad approaches to data protection and informational privacy. These include foreign legislations, judicial precedent and existing and proposed legislative efforts.

Part-2

- **Scope and Exemptions**(Pg 24-75): specific issues such as the applicability of a data protection law to a geographic area (national and international), types of people (natural and artificial such as companies), the definition of personal data itself and to whom such a law (data controllers) should apply.

Part-3

- **Grounds of processing, obligation on entities and individual rights**(Pages 78-141): Includes basic data protection principles on data processing i.e. notice and consent. It also contains comments on the limitations on processing and exceptions to this rule (public interest). It also contains storage limitations ,comments on data quality and the right to be forgotten.

Part-4

- **Regulation and Enforcement**(Pages 143-203): How (for eg. co-regulatory models that require codes of practice) and by whom the data protection framework will apply. It also invites comments on penalties on the nature of compensation and criminal offences.

Part-5

- **Summary** (Page 204) : Seven key principles are identified which are most important and form the backbone of the consultation.

Seven Key Principles

	Brief
1	**Technology Agnosticism** : "The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance."
2	**Holistic Application**: "The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims."
3	**Informed Consent** : "Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. The law must ensure that consent meets the aforementioned criteria."
4	**Data Minimisation** : "Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject."
5	**Controller accountability**: "The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing."
6	**Structured enforcement**: "Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralized enforcement mechanisms."
7	**Deterrent penalties**: "Penalties on wrongful processing must be adequate to ensure deterrence."

Thanks