Privacy and Personal Data Rights

How people may violate them inadvertently in computing endeavors and why you should not let this happen

Prof Jorge Sanz

Week 2 (classes on January 21) and *Week 3 (classes on January 28)*

Topics – for Week 2 and Week 3

- Introduction - A bit of background on your lecturer professor
- The promise of a *Data Economy Era*
  - Reality or IT vendor / government / techy illusion ?
  - How Big Data augments the concerns and issues about privacy
- Personal Data: Individuals' rights and enterprise obligations
- Challenge yourself
  - Personal consequences: *You don't know what you do not know*
  - Business consequences: *What it may be illegal in your business-IT ideas*
  - Societal consequences: *Damages and implications beyond the individual*
- Concepts on Privacy
- Asymmetries in the times of Personal Data
- Singapore, Europe, China and the US
- The *right-to-be-forgotten*
- Beyond the present laws: Anticipatory / Inferential techniques
- Examples of T&Cs usually requested in enterprise contracts
- Recommended reading and more literature

Career Journey

1981 — PhD University of Buenos Aires

1982 — Assistant Professor University of Illinois at Urbana-Champaign (tenured in 1985)

1985 — IBM Research California

1991 — IEEE Fellow

1993 — Full Professor University of Illinois at Urbana-Champaign

1994 — IBM Director New Technologies for LA Telecom New Business (1996)

2000 — President University of Saint Andrews (Buenos Aires)

2003 — IBM Almaden Research California

2012 — Chief Innovation Officer Banking Industry IBM Corporation

2013 — Full Professor Business School and School of Computing (on-leave)

Director Business Analytics Center National University of Singapore (NUS)

2017 — Luxembourg Scientific Director Analytics and Regulatory Technology

2018 — Full Professor Business School and School of Computing

Data Economy Era: A real opportunity …

"Data Monetization": Making money with Data

- Data comes in many forms; varies with the LoB and industry
- Value is not only intrinsic to digital footprints but around **ANALYTICS** used

- **Data affects all Lines-of-Business**

  F&A, HR, SC, Marketing, IT, Sales …
- **Data impacts all industries**

  Finance, Manufacturing, Retail, Telco, Government …

- **IDC Big Data Analytics (*HW + SW*) Market Projection**

  Based on $ 160 B in 2017 … $ 210 B in 2020
- **European Commission Estimate of *Data-driven Market***

  +600 Billion – 1 Trillion euros yearly in 2020

Many forms of *data* involved in the Data Economy

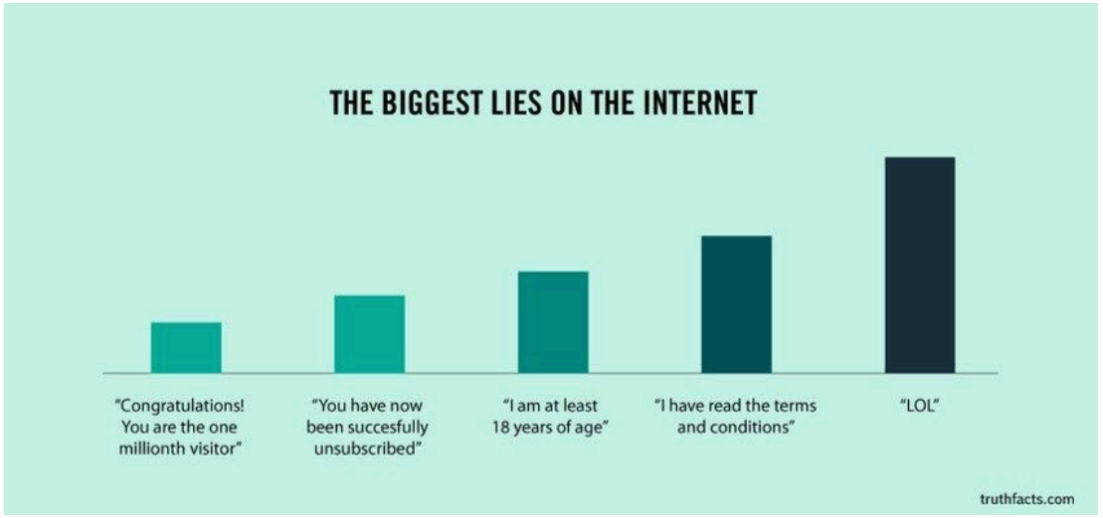
- Some data are obviously personal …
  - Name, date of birth, domicile, etc.
- … not all data relate to an individual …
  - Sensors in manufacturing, traffic signals in the streets, weather information, monthly revenue from your family business, number of failed daily deliveries by Sing Post … **are *not personal data***
- But other cases fall within a *digital space* that compose the extension of a person in daily life …
  - How about your phone GPS location ? … your bank account balance ? … your driving pattern recorded from a device inside a car rental ? … the result of a diabetes or HIV test ? … what you say about yourself in a public website … ?
  - Guess an answer for the above cases …

Big Data brings more challenges for privacy law and enforcement

- Enterprises, Global Companies and Governments are facing renewed and unique pressures with privacy issues arising from **Big Data applications**

arrival make worse

- The advent of Big Data exacerbates privacy concerns due to pervasive collection practices of personal information carried out by most enterprises over digital channels …
  - Problems involve *Employees and Individuals*
  - Different jurisdictions with different laws
  - Different industries with distinct regulatory frameworks
  - … and these concerns are just "the tip of an iceberg" in the light of *predictive techniques used to infer private information not released by individuals in unconsented practices*



Hundreds of things happen around Privacy …

But they put you as an "spectator"

Cambridge Analytica Facebook Scandal

Cambridge Analytica closing after Facebook data harvesting scandal

Political consultancy, under fire over use of millions of Facebook users' data, has begun insolvency proceedings

▲ Cambridge Analytica is closing its doors. Photograph: The Washington Post/Getty Images

The company has been plagued by scandal since the Observer reported that the personal data of about 50 million Americans and at least a million Britons had been harvested from Facebook and improperly shared with Cambridge Analytica.

Cambridge Analytica denies any wrongdoing, but says that the negative media coverage has left it with no clients and mounting legal fees.

▲ What is the Cambridge Analytica scandal? - video explainer

You as the ACTOR: Challenge yourself, I

- 99.99 vs 0.01 rule ➔ Happy path is sweet, until something happens…
  - I have never read Google's or Facebook's terms-and-conditions and if they screw me, I will fight them in Singapore Court …
- No one reads terms-and-conditions. After my customers click "ok", we will be safe to move on with our biz activities …
  - Since they consented, if they try to screw me then, it will be an easy-walk for me in Singapore Court …
- If bad comes to worse, I will just use pseudonyms or I will strip off names and addresses …
- Singapore is more "lenient" than other other places so I can set my data-business here and offer services to the world … If I breach, all fines in Singapore are very cheap, so ? …
- If anyone is unhappy with my service, I will erase all their content and terminate the service … so what ?

You as the ACTOR: Challenge yourself, II

- My business partner lives in California, we can move our servers and make the entire service from there, big deal ...
- I can safely process in Singapore data from Chinese, Europeans and US Citizens for my start-up …
- In order to reduce costs for my company, we will do all our data processing in Calcutta, with my student pals from India …
- Personal Data Protection law in Singapore replaces all industry regulations on personal data and related privacy matters …

OK, Prof I got it …

- We will hire an attorney not to be illegal, thank you for your advice; now let us go out of here and eat … ☺

➔ The point is very different …

- You will seldom innovate EFFECTIVELY without **knowing** the key constraints … It is all about the power of **YOU** knowing …
  - ✓ I know **<u>hundreds</u>** of examples of ”great biz-tech ideas” that fail / would fail because of breaching privacy (information privacy and / or privacy beyond info)
  - ✓ It is about ethics, positively. But it’s also because not being naïve or silly is equally important. I want to INSPIRE YOUR BEST CREATIVITY and THINKING EFFECTIVELY
  - ✓ The Tutorials will cover some of these grounds and we will work in smaller groups on cases (real cases) and walking the talk into real action

- Lastly … people call attorneys (mostly in SMEs, non-profits, Gov enterprises, NGOs, family business, startups) *after they screwed*

Example: *The Social Radar*

- You in Singapore and your student pals in the US and Europe want to launch a new service startup
- The team aims to design a great new family of NLP / NLA in 15 languages and Image / Video pattern recognition based on some very promising techniques that the team will develop
- Your plan is to scan massively the web for public sites and pay top Media Aggregators for their renting all data from their subscribers to you
- Your algorithms are so good that they can match the majority of blogers and other internet users directly to their identity known in the Aggregators.
- Your algorithms also to produce a rank of "*likely trustable customers*"
- Your idea is to offer all Finance, Insurance, Telco Services companies in the world an **API**: You will receive the customer name and some basic customer data and you will return a "social score" indicating how "suitable" or "trustable" the client is
- You plan to charge per API call. Your exit strategy is either to be acquired by a Bank or a major Telecom, or to break even and go to NYSE for IPO

Is there any no-go here ?

What is special about privacy specifically associated with computing ?

Amount of personal information that can be collected

Speed at which personal information can be transmitted

Duration of time that the information can be retained

Kind of information that can be acquired and exchanged

Four kinds of practices that threaten privacy

- Data gathering techniques
  - ✓ IoT, smart devices, sensors, cookies, RFID, etc.
- Data integration techniques
  - ✓ Extracting information from two or more related databases that contain information about individuals, and integrating that information into a composite file
- Data mining techniques
  - ✓ Consumer profiling
- Data processing techniques
  - ✓ IT Outsourcing services involving processing of personal data

Different Views and Role-Players related to *Data*

Citizens

Enterprises

Awareness View

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

PDPC / IMDA in Singapore

Rule, Educate Enforce, etc.

Regulators

GDPR / PDPA / CSL Industry Acts

Private Contract Law

Copyright & Sui-Generis Rights Laws

GRC Views

Methods & tools

Privacy Process Capability Assessment

DPO

Methods & tools

Business Process Privacy Assessment

Business Line Manager

Asymmetries across Jurisdictions (I)

China Singapore India

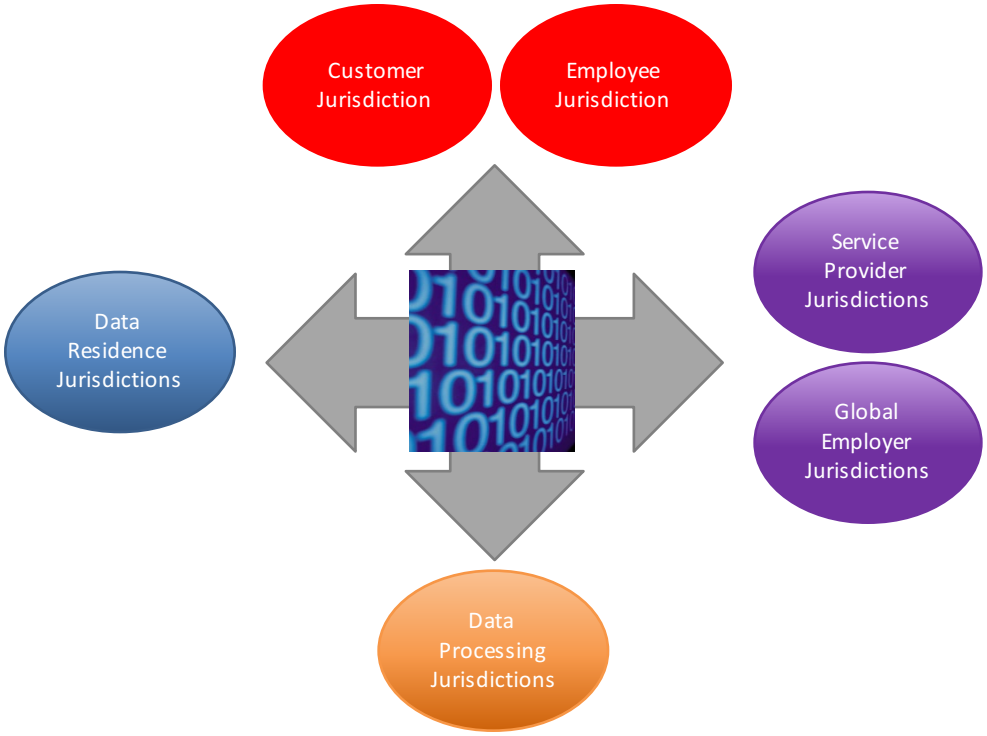
Spectrum on Similarity of Data Protection

EU
Single legislation on personal information implemented in 2018

Safe Harbour

EU-US Privacy Shield ?

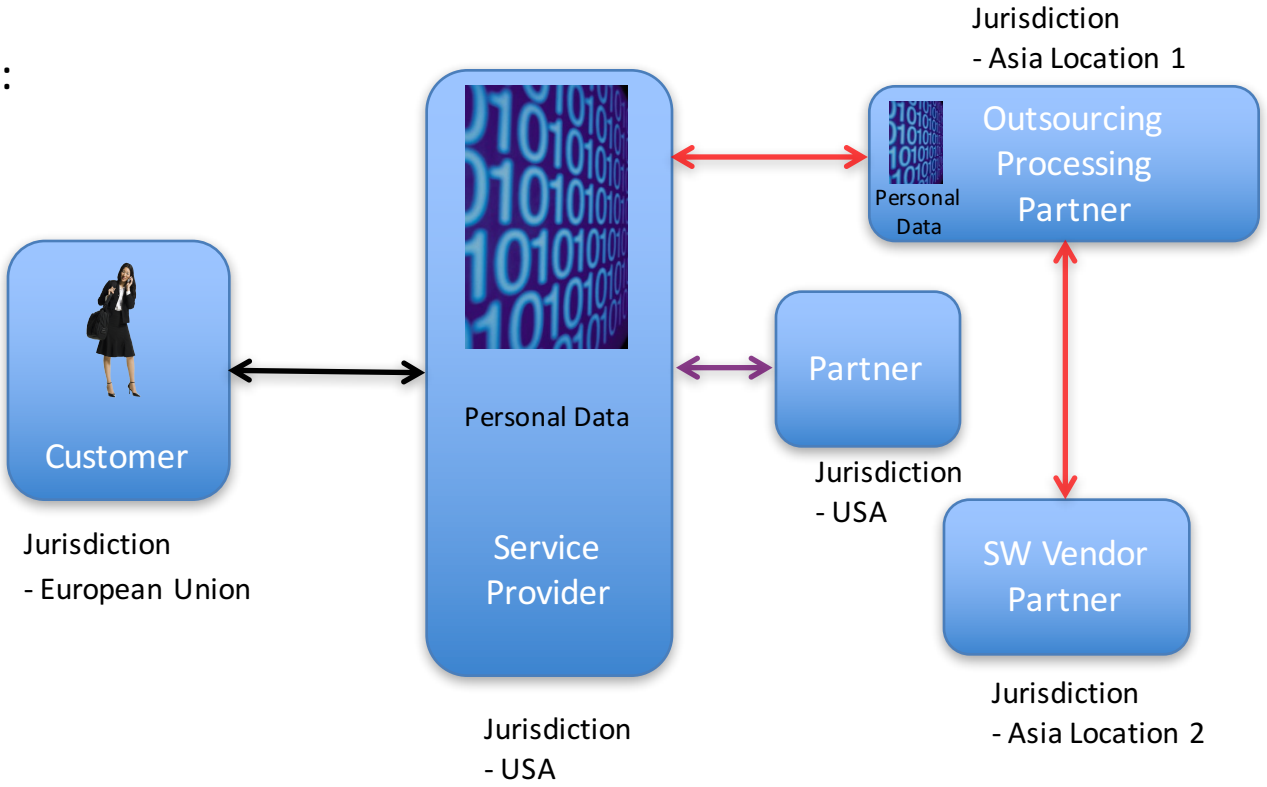
US
There is no unified legislation on personal information and no single authority to oversee compliance



- The tension across jurisdictions in the control of privacy rights is explained by the complex, nature of big data collection, processing and storage
- A number of different laws and regulatory frameworks maybe at stake in preserving privacy of individuals

Asymmetries across Jurisdictions (II)

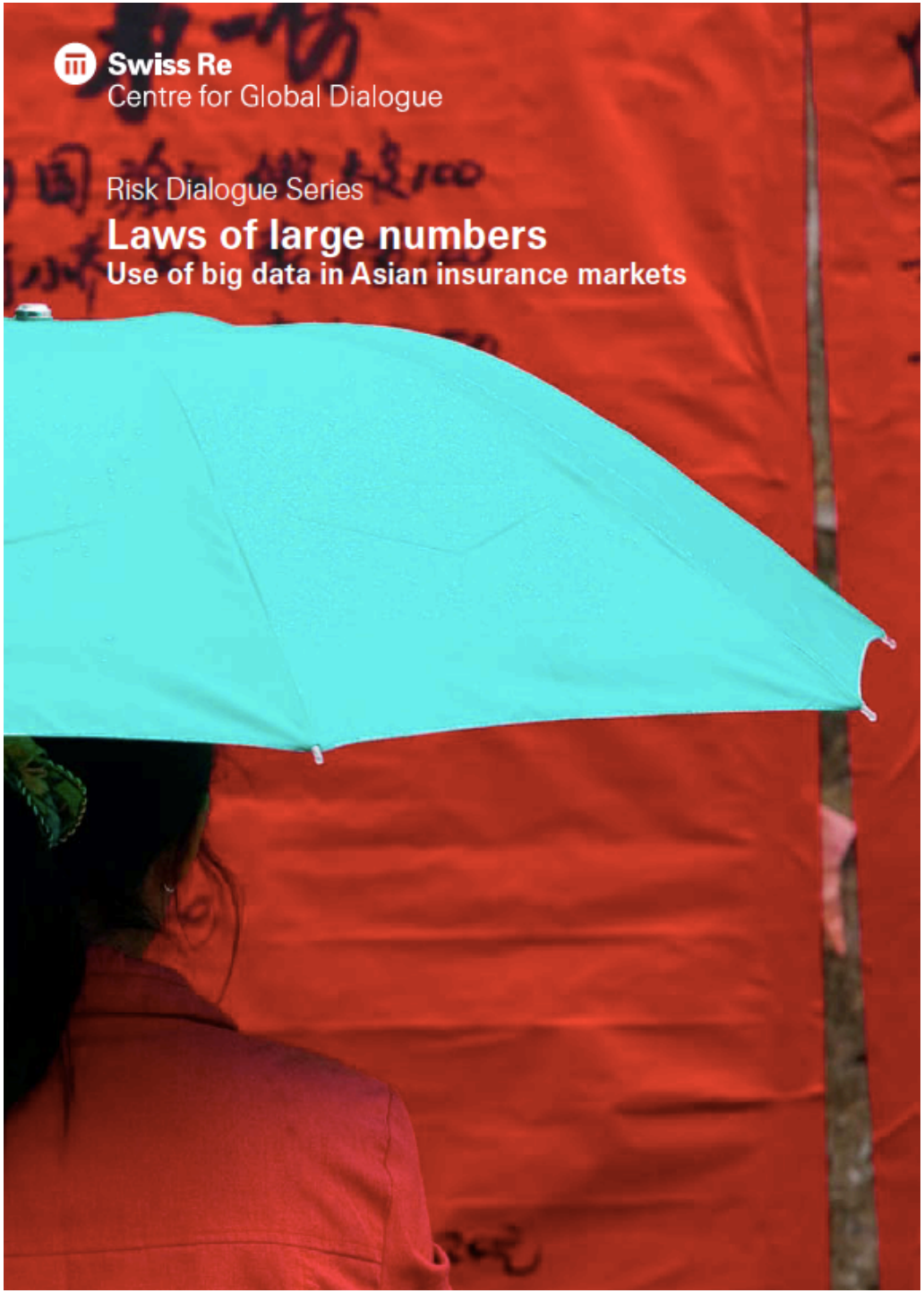
Example:



Discrepancies across Private Data Protection Acts impact on Asian countries

- Poses threat for growth
  - Jurisdiction of the outsourcing vendor may or may not respect the privacy rights of the jurisdiction where the collection of data from customers took place

- But its is also an opportunity in the Data-Economy
  - With local laws in Asia that incorporate the needed changes to fit the specific conditions, countries can be "safe home" for data-related work



Big Asymmetries in the Era of Big Data

Jorge Sanz - Janet Chow

2015

Paraphrasing Bill Clinton's US Presidential Campaign in 1991 …

It is the algorithm, stupid !

Moving into more serious Asymmetries

Information derived / inferred without the knowledge of individuals

Have people "consented" to this practice?

Capabilities to "infer" personal information about people

- Breaching the privacy right of an individuals who may never have voluntarily provided or consented that any entity would be authorized to infer.

Source of picture from http://www.mirror.co.uk/news/uk-news/june-birthdays-happiest-november-milestones-5792686

Example:

Joe (wearing grey shirt) attended a birthday party and posted the following picture on his Facebook page with a comment *on 28 Sept*:

"What a wonderful party yesterday night. Happy Birthday to Rachel Wilson ! Wishing you lots of happiness and kudos for getting that promotion tomorrow!"

So much we can infer about this picture, right?

The *Black Box* … (Analytics, AI, Machine Learning)

What happens when techniques for disorganized complexity phenomena are used for phenomena of organized complexity ?

More on this subject later in this course

Automated Decisions - *GDPR says NO !*

The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is ***based solely on automated processing*** *and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices* ***without any human intervention****.*

Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.

Back to concepts: *Privacy* and its Meaning

- A broad definition of the **Right of Privacy** is "the right to be let alone"
- Privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs
- Privacy can be divided into the following separate, but related, concepts:

(i) **Information privacy**, which involves the establishment of rules governing the collection and handling of personal data. It is also known as data protection

(ii) **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches

(iii) **Privacy of communications**, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and

(iv) **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space and includes searches, video surveillance and ID checks

Information Privacy

Personal Data Meaning and Relevance

- The term "personal data" means to describe not only information that is used to identify a person (such as her birthdate, address, Social Security number, etc.) but also digital content that refers to a person, such a photographs or writings by or about her

- However, things are a lot more complex (and also at times ambiguous) as we will see soon …

Personal Data Protection Acts

What are Data Protection Acts (Regulations or Laws) ?

- Regulatory frameworks and legislation that have been put in place with the main intent to protect individuals against **misuse** or **abuse** of personal information
- Regulations include mechanisms for establishing supervisory authorities and may require organizations to designate a point-person for responsibility with compliance
  - Institutions are required to appoint a Data Privacy Officer (DPO)
- Regulations usually establish penalties for organizations not complying
  - In some cases quite severe, like in Europe and China

Scope of Personal Data Laws

- Most countries / regions have their own Personal Data regulations (laws, acts)
- All these regulations generate related compliance processes and practices by firms (profit and non-profit, including government agencies)
- However, none of these laws apply to …
  - Data about individuals handled in household-like personal and family activities
  - Data in the concert of criminal law and related procedures is not included either

Different jurisdictions with similar and dissimilar Personal Data *principles* and laws

- Four examples used in this course …
  - Singapore
  - European Union (28 states)
  - China
  - United States

➔ Any business / enterprise endeavor in computing that you participate in or you may start up will likely face dilemmas and issues with these principles and laws

  - The more global or extended the activity, the more prone to violations and penalties
  - The foundational beliefs behind the laws are not identical, so interpretation of what constitutes a violation is also a challenge
  - Above and beyond *risks*, there is an ethics behind activities involving the collection and monetization of personal data

Personal Data in Singapore

What is Personal Data for Singapore Law ?

Personal Data:

- Data that **allow identification**, either alone or in combination with other data sources potentially available involving the same individual

Sensitive Personal Data:

- Information related to "sensitive" facts such the health of an individual, religion, race, personal beliefs, …

Personal Data in Data Protection Acts

From the European Law, called GDPR

Article 4

'Personal data' means any information relating to an identified or identifiable natural person ('data subject')

An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an *online identifier* or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

GDPR includes the term 'online identifiers' within the definition of personal data

- These may include information relating to the device that an individual is using, applications, tools or protocols:
  - internet protocol (IP) addresses
  - cookie identifiers
  - other identifiers such as radio frequency identification (RFID) tags.

- Other examples of online identifiers that may be personal data include:
  - MAC addresses
  - advertising IDs
  - pixel tags
  - account handles
  - device fingerprints

Personal Data in the UK

The UK's Information Commissioner's Office explains:

"*By itself the name John Smith may not always be personal data because there are many individuals with that name. However, where the name is combined with other information (such as an address, a place of work, or a telephone number) this will usually be sufficient to clearly identify one individual.*"

"Simply because you do not know the name of an individual does not mean you cannot identify that individual. Many of us do not know the names of all our neighbours, but we are still able to identify them."

Controllers and Processors

Some legislations distinguish the role of the responsible party / parties for collecting and managing personal data (Controller) from the party / parties that may be processing personal data on behalf of the Controller (Processor) …

- Singapore
- European Union
- … But not China or the US

➔ If someone was thinking that "processing" could be a separated legal concern and thus, freeing data gatherers from anything done when processing the said data … ☺

Personal Data or Not Personal Data ?

Example

At New Year celebrations in Orchard Street two almost identical photographs of the revellers are taken by two separate photographers and stored in electronic form on computer.

The first photographer, a photo journalist, takes a picture of the crowd scene to add to his photo library. The second photographer is a police officer taking photos of the crowd scene to identify potential troublemakers.

The data in the electronic image taken by the journalist is unlikely to contain personal data about individuals in the crowd as it is not being processed to learn anything about an identifiable individual. However, the photo taken by the police officer may well contain personal data about individuals as the photo is taken for the purpose of recording the actions of individuals who the police would seek to identify, if there is any trouble, so they can take action against them

Personal Data or Not Personal Data ?

According to the UK interpretation …

Data may not be personal data in the hands of one data controller (for example, the estate agent) but the same data may be personal data in the hands of another data controller (for example, the police) depending on the purpose of the processing and the potential impact of the processing on individuals