Pacific
E-commerce
Initiative

Data Disciplines:
Cross Border Data Flows

E-Commerce Training Programme
for Pacific Negotiators
March 28 – April 1, 2022

PACIFIC ISLANDS FORUM

Cross-Border Data Flows

The global economy increasingly relies on free flow of data.

Are there legitimate purposes for Government to restrict cross-border data flows?

Cross-Border Transfer of Data & Data Localization

DATA LOCALIZATION: Can countries require that data is stored within their borders?

In recent years, some countries have imposed a legal requirement on companies to store data (or at least copies of data) within the country.

Arguments for Data Localization requirements

- To protect or improve citizens' privacy
- To ensure rapid access to data by law enforcement officials.
- To protect or ensure national security
- To improve economic growth or economic competitiveness

Arguments against Data Localization requirements

Data localization requirements:

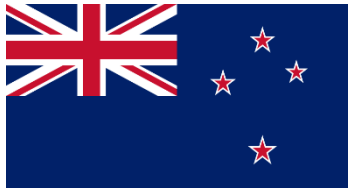
- increases costs and risks for national (and investor) companies – e.g. to build infrastructure.
- reduces ability of services/companies that rely on data e.g. accounting software for small business
- Reduce trade and overall economic growth (Brookings Institution)
- Does not increase privacy/data access/national security, as data is not stored efficiently

WTO e-commerce negotiations: Location of Computing Facilities

DATA LOCALIZATION: Can countries require that data is stored within their borders?

Indonesia mandates that data must be stored on servers in the country, but now only for 'public services'. Private servers must be open to 'supervision'.

Cybersecurity Law of 2019 requires all forms of personal data belonging to Vietnamese citizens to be stored locally, but now restricted only to companies notified that they have violated Vietnamese laws.



New Zealand's Internal Revenue Act requires businesses to store business records (such as tax) in local data centers.

WTO e-commerce negotiations: Data Localization

DATA LOCALIZATION: Can countries require that data is stored within their borders?

Data Localization negotiations at the WTO are split. This may turn into one of the major barriers to concluding an e-commerce Agreement.

The negotiations should not include the issues of data flow or data storage or treatment of digital products at this time, due to differing views of Members.

"Members **shall not** require the use or location of computing facilities in its territory as a condition for conducting business in that territory" except "a **legitimate public policy objective**".

"No Party shall require a [person] to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory"

Cross-Border Transfer of Data: Policy Questions

General Obligation on Data Transfer ?

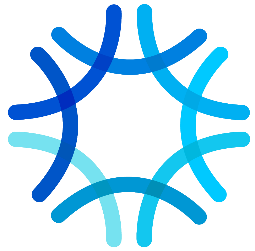
Should a global agreement include an obligation (or preference) for laws that secure free flow of data across borders?

Data Localization ?

What position should Governments take on 'location of computing facilities'?

Sectoral Approach?

Should certain sectors be excluded from obligations on data flow?
Financial Services?



Pacific
E-commerce
Initiative

Society of International Economic Law (siel) | Università Bocconi MILANO

Rethinking Global Economic Governance
7 – 9 July 2021

DO EXCEPTIONS PROVE THE RULE: An inquiry into the exceptions to the [commercial] data flow rules in the WTO JSI on E-commerce

Leonila Guglya, LL.M, SJD. PhD
SwissLegal Rouiller et Associés (Geneva) / guglya@swisslegal.ch/

I. Cross border commercial data flows: an introduction

Cross border flow of data – *an exhange of information between computer servers located in different states* (1) – is indispensable for the international trade.

Establishment of the **common data flow rules** could contribute to predictability and cost-efficiency of international trade, benefiting all – businesses (notably, MSMEs) and consumers.

Rules addressing cross-border data flows are incresingly elaborated nationally and included into the PTAs. However, some jurisdictions (mostly developing countries/ LDCs) have no data rules yet (2) and **unilateral** data transfer authorization measures are widespread (3).

The dedicated disciplines [typically] are:

- **Unrestricted flow of commercial data**;
- The **prohibition of** the requirements to process and / or store data on the territory ("**data localization**" or "data centre localization") as a condition for doing business in such territiry;
- Specific rules applicable to the **flow / localization of** sectoral (commonly – **financia**l) **data**

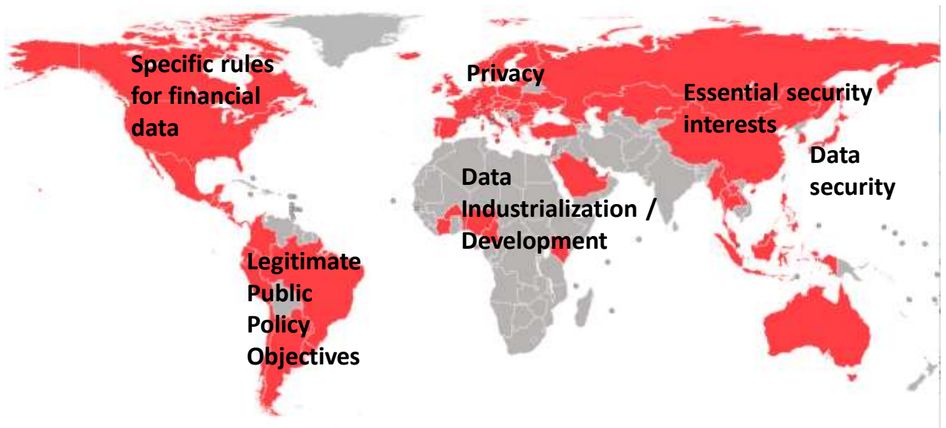
II. The WTO Joint Statement Initiative (JSI) on E-Commerce

The WTO Joint Statement Initiative (JSI) on E-commerce was launched in 2017, first as an exploratory forum [*additional to the WTO Work Programme on Electronic commerce, 1998*], and, next, since 2019, as a forum for **plurilateral negotiations**, now counting **86 Participants**. The JSI remains [largely] open to non-participating WTO Members, but, it lack broader transparency.

The JSI is the *most representative "laborarory" developing modern global e-commerce rules.*

The JSI aspires establishing rules on the cross-border data flows, even if *not all the Participants support such rules*.

III. Proposed exceptions: mapping and an overview



Author, based on (4). The territories of the Participants of the JSI are marked red. The mapping of the exceptions does not fully reflect the geography of their [often numerous] proponents

The **exceptions reflect varied interest and objectives**, often also found in the domestic legal and policy frameworks of their proponents and/ or FTAs, in which they take part.

The GATT and the GATS exceptions' models are not followed.

While the "**privacy**" – "**security**" - "**legitimate public policy objectives**" trio is best known, other or elucidated in more detail, concerns, such as **data industrialization, data security**, as well as **specific exceptions to the rules fo**r certain sectoral [**financial**] **data**, were also added.

References: (1) R.F. Fefer, Data Flows, Online Privacy, and Trade Policy, CRS Report R45584 of 26.03.2020, available here; (2) L. Guglya, M. Maciel, Addressing the Digital Divide in the Joint Statement Initiative on E-Commerce: From enabling issues to data and source code provisions, CUTS International and IISD, Geneva, 12.2020, available here; (3) OECD, report of the Working Party of the Trade Committee: Mapping commonalities in regulatory approaches to cross-border data transfer, TAD/TC/WP(2020)15/FINAL of 23.04.2021, available here; (4) WTO E-commerce Negotiations: Consolidated Negotiating Text – December 2020, Revision, INF/ECOM/62/Rev.1, of 14.12.2020, available here. In part, the analysis is based on the submissions of the Participants of the WTO JSI on e-commerce, not made accessible to the public.

IV. Proposed exceptions: analysis

Ex	The essence	Status quo / Peculiarities	Im-t*
Privacy	The exception allows *restricting cross border data flows when equivalent* (even if not identical) *protection of personal data at the destination could not be ensured*. The "protection" might imply limiting both – private and public (regulatory) access to personal data.	Definitions, scopes, extents of protection of personal data vary. Unilateral measures authorizing cross border transfers prevail. Data segregation / depersonalization might be unavailable / costly. GATS Art. XIV preliminarily justifies measures protecting privacy. Members allocate different value to privacy, with some seeing it as a "fundamental right", others – among the public policy objectives.	MAJOR
Security	The exception, presented without sufficient precision, might allow a Member *to restrict data flows if this is necessary for addressing* [potential[*security hazards.*	"Security" appears to justify censorship practices and an overall state control over the foreign data, impacting predictability. It is not yet clear how the "necessity" element included in the text of the exception, would be implemented or interpreted.	MAJOR
Data Security	The exceptions addresses the situations in which *private or business data risks third party interference.*	National data security rules and institutions vary in maturity and are often better adapted to ensure integrity of the data saved on physical media. This exception is not explicitly proposed, but the relevant concerns are voiced in the discussions of the other rules.	MAJOR
Public Policy	The exception allows *restrictions to meet legitimate public policy objectives subject to the 2 safeguards*: a) a measure should not be applied in a discriminatory manner; b) it should not impose restrictions greater than [necessary/required].	Policy objectives pursued by the Members resorting to cross-border data flows restrictions indeed vary. The exception appears to integrate the "light" adaptation of the chapeau of the GATT/GATS general exceptions.	SIGNIFICANT
Development	The *[permanent]* exception is aimed at *allowing developing counties to build capacity and skills in data storage and processing*, permitting them not to comply with the data flow rules.	The data infrastructure in most of the developing countries is absent, nascent, or is being developed. At least one PTA (RCEP) provides LDCs with a transitional period for implementation of the data flow rules.	MAJOR [if not transit.]
Financial data	The exception establishes specific rules for the "remedial" localization of [certain] financial data. Such is allowed if "*immediate, direct, complete, and ongoing*" access [to the data processed or stored abroad] by the financial regulator could not be ensured, or when *the regulator is unable to access data for financial regulation / supervision*.	Financial data is exempted from the scope of "digital" chapters of several PTAs (such as USMCA, CPTPP, RCEP, ASEAN ECA). Data localization measures are often used in its respect. The discipline might cause "*remedial*" localization of financial data stored / processed in the developing countries and LDCs due to their inability to ensure sufficient access thereto at all times.	NOTICEABLE sectoral impact

Author, based on (4). * MAJOR: Might deprive the disciplines of their effect; SIGNIFICANT: Effect somewhat minimized by the safegurads; NOTICEABLE: might have impact on of effect of the disciplies in particular sectors / on certain groups of Members.

V. Reflections and the way forward

The **data flow disciplines are yet not ripe** neither on plurilateral, nor (by and large) on the regional level, since most of the **exceptions**, if resorted to, **deprive the rules of their actual effect**.

Progress on some among the 40+ topics on the JSI Agenda, notably those belonging to the *Focus Groups C (Trust and digital trade / e-commerce)* and *D (Cross-cutting issues)*: **Online consumer protection, Spam, Protection of Personal Information, Source Code, ICT Products that use Cryptography, Cybersecurity** and **Technical Assistance and Capaciity Building**, might contribute to alleviating of the need to resort to certain exceptions through enhancing **trust** between the nations and their data protection authorities.

Elaboration of the **comon data taxonomy** (the *"HS" for data*) might improve predictability of application of the privacy exception.

The ongoing WTO dispute settlement crisis might limit the role of the WTO DSM in interpretation of the new exceptions (NB: some of the PTAs subject such exceptions to self-judging or exclude all e-commerce rules from the dispute settlement outright). Thus, **better elucidation of the exceptions** already at the drafting phase could be useful.

Phasing out restriction on the cross border flow of commercial data, when imposed through the exceptions to the rules, might take time and efforts, being based on **cooperation** of different scope and scale, paving way to a universal result through *incremental steps.*

Pacific E-commerce Initiative

Consumer Trust: Online Consumer Protections

E-Commerce Training Programme
for Pacific Negotiators
March 28 – April 1, 2022

PACIFIC ISLANDS FORUM

Data Disciplines & Consumer Protection

The **EXPLOSION** of new data creates challenges for Government, Business and Consumers

Consumer Protection:

Do consumers have the same protections as in the real world?

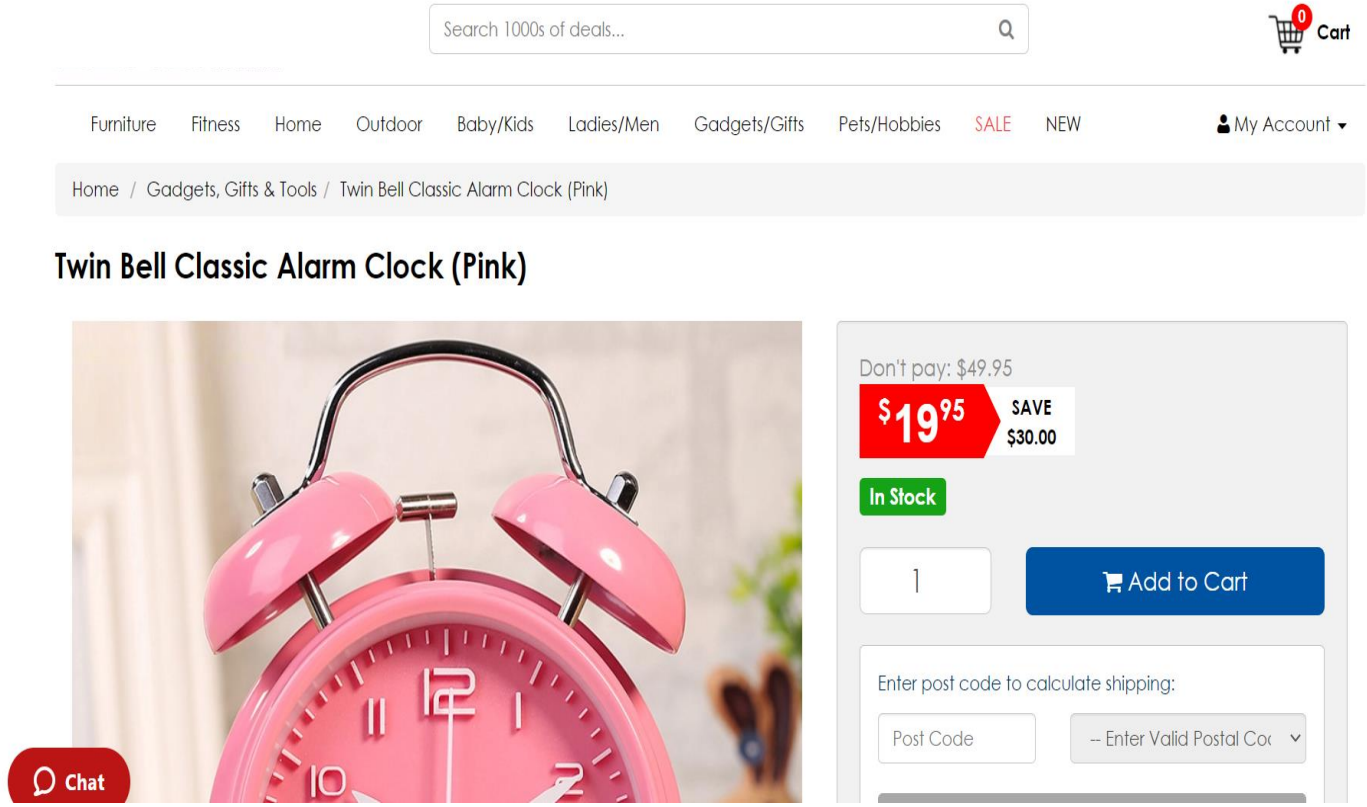
Data Protection:

How to secure and protect personal data?

Cross-Border Data Transfer:

How do Governments respond to movement of data across borders?

Offline and online consumer protection



No misleading, fraudulent or deceptive commercial conduct

Consumer Protection Disciplines

PROTECTIONS:
Do consumers have the same protections as in the real world?

Just like in the offline world, online consumers rely on rules that protect them.

- What information must be provided to consumers?
- How are disputes settled, and refunds/exchanges made?
- How to protect against unsolicited messages (aka 'SPAM')

Most common approach:

- **'Information'**: New laws require all information necessary for customers to make informed decision, including: identity of seller, terms of purchase/exchange/refund, quality of goods/services.
- **'Misleading information'**: normal laws apply – online sellers cannot mislead their customers.
- **'Dispute Settlement'**: new mechanisms for online dispute resolution. How do these apply across borders?

SPAM

"High volumes of spam consume valuable network resources, and are a particular burden on countries with limited Internet access and bandwidth." (Internet Society Policy Brief)

- "Unsolicited Commercial Electronic Messages" = SPAM
- Disciplines include:
  - Require senders to self-identify
  - Require senders to obtain consent
  - Require senders to allow opt-out
- Global rules can help coordinate crack down on SPAM senders wherever they are
- But how would rules be enforced?

Consumer Protections: Policy Questions

Laws for online consumer protection

Mandatory?
'Best Endeavours'?

Online Dispute Resolution

What is status of alternative dispute resolution in other areas of commerce?

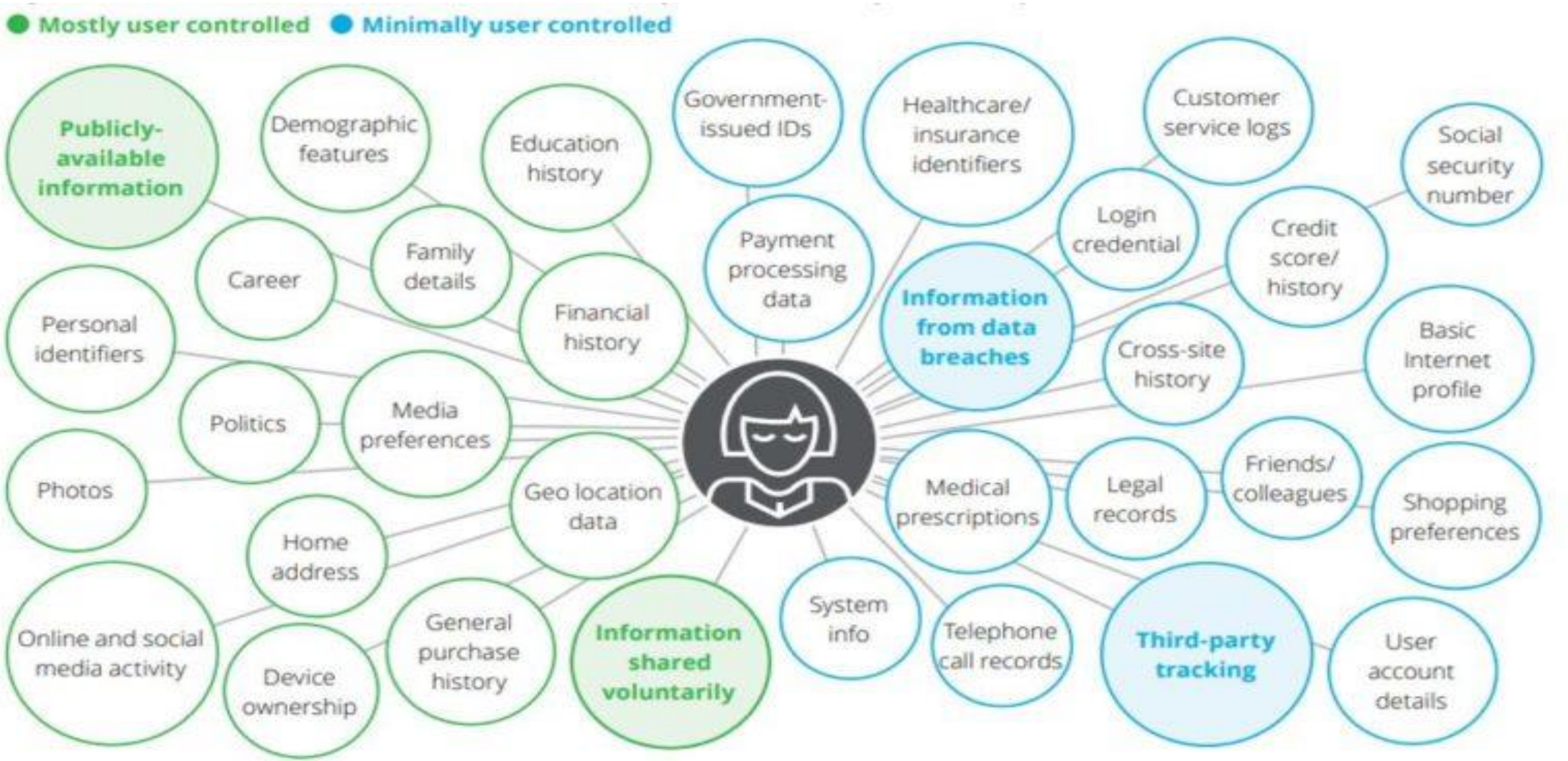
What level of commitment would reflect interests of citizens?

SPAM

What is a reasonable commitment on SPAM?

What level of commitment would match enforcement capability?

Personal Data Protection



Source: Deloitte

Personal Data Security & Privacy

Data Privacy

Compliance with data protection laws and regulations. Focus on how to collect, process, share, archive and delete the data

≠

Data Security

Measures that an organzation is taking in order to prevent any third party from unauthorized access.

Consent of the Consumer for collection, use, storage, disclosure etc.

Take reasonable steps to prevent misuse, loss, unauthorised access etc.

Personal Data Security & Privacy: Policy Questions

Nature of Personal Data Laws

Mandatory?
'Best Endeavours'?
International Standards?

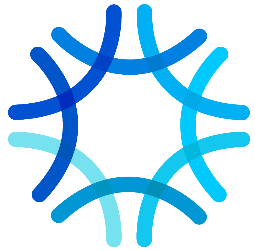
Govt use of Data

Should Governments be subject to same disciplines?

How to protect citizens from their Government's use of data?

Cross-Border Data?

How should countries regulate privacy & security obligations when data crosses borders?



Pacific
E-commerce
Initiative