


A network diagram of white person icons connected by thin white lines, overlaid on a background of hands holding a smartphone. The icons are arranged in a roughly circular pattern with some internal connections.

Giving consumers clarity and control over the use of their online data

Philippe Moura
Regulatory Manager
GSMA

A horizontal bar at the bottom of the slide, divided into a red section on the left and a teal section on the right.



Mobile Safety, Privacy and Security

Building trust and transparency across the mobile ecosystem

... address consumer protection issues related to illegal and harmful activities

... protect the underlying infrastructure



... protect and respect consumers' privacy interests and enable them to make informed choices

... comply with public safety obligations while being supportive of human rights concerns

Source: GSMA, "Safety, privacy and security across the mobile ecosystem: Key issues and policy implications," February 2017



Protecting Consumers

Mobile Industry Principle



Operators will take proactive steps to address consumer protection issues related to illegal and harmful activities linked to or enabled by mobile phone usage, by:

Working collaboratively with other agencies

to deliver appropriate multilateral solutions

Implementing solutions designed to prevent use of networks to commit fraud or criminal activity

and devices being used in ways that harm the consumer

Educating consumers on safe behaviours

to build their confidence when using mobile apps and services



A Multi-Stakeholder Effort Is Required

To Protect Consumers and Encourage Safe and Responsible Use

Governments and law enforcement agencies

Ensure appropriate **legal frameworks, resources and processes** are in place to deter, identify and prosecute criminal behaviour

This often requires global cooperation

Mobile network operators

Remind consumers to be **aware and vigilant**, and encourage them to use the full suite of security measures available

Other industry ecosystem players

Help **protect consumers** when they are using mobile devices and services

Educate them about safe behaviours and good practices



Protecting Consumer Privacy

Mobile Industry Principle



Operators will take proactive steps to protect and respect consumers' privacy interests and enable them to make informed choices about what data is collected and how their personal data is used, by implementing policies that promote:

Storing and processing personal and private details securely

in accordance with legal requirements where applicable

Being transparent with consumers about data that we do share

Anonymised and in full compliance with legal requirements

Providing the information and tools

for consumers to make simple and meaningful choices about their privacy



We Face a Number of Challenges

Consent fatigue, which intensifies as the number of devices and services people use increases

New use of data long after it was collected, which can make notice or consent impossible or disproportionate

Delivery of meaningful and timely information to users

Displaying T&Cs on small screens, applying them to IoT and drones, and considering data localization scenarios



Privacy in Practice

GSMA Mobile Privacy Principles*

Openness, transparency and notice

Security

Purpose and use

Children and adolescents

Data minimisation and retention

Accountability and enforcement

Forming the basis of all context-specific guidelines and privacy best practices

Mobile App Development

Published guidelines including:



- Location
- Data retention
- Education
- Social media
- Mobile advertising

Big Data and Privacy

Considerations for data handling and use, including



- Privacy impact assessments
- Access to data sets
- Cross-border data transfers
- Ethics

Mobile Connect

User-centred model — privacy by design, including:

- User choice and control
- Data minimization
- Purpose and use limitations



Other Contexts

The GSMA inputs on privacy issues for many contexts:

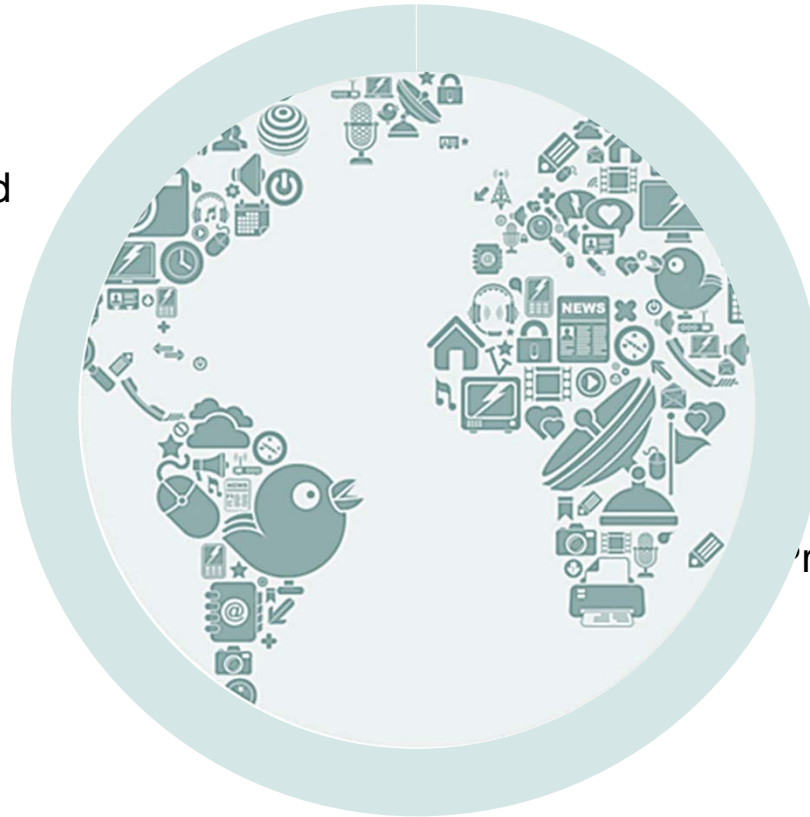
- Machine-to-machine
- Internet of Things
- Children's privacy
- And more



Cross-Border Data Flows

More people are online, generating more demand for goods and services offered across borders

Newer technologies are dependent on cross-border data: Internet of Things, connected cars, machine-to-machine, drones, etc.



Privacy concerns are broadly similar

Privacy principles are broadly similar

Promoting skills, solutions, innovation

ECONOMIC GROWTH

SOCIETAL BENEFITS

Data Localisation Requirements

TURKEY

Public communication network and service providers are prohibited by law from transferring customer call data outside the country (with exceptions for roaming and international call details)

RUSSIA

Russia recently signed a law requiring all entities in Russia collecting the personal data of Russian citizens through electronic communications (including subsidiaries and branches of foreign companies) to store it in databases located in Russia.

CHINA

Companies in some business sectors, for example banking and healthcare, may not transfer customer data overseas without explicit user or regulatory permission. Critical information infrastructure operators, including in the finance sector and public utilities companies, are required to store data collected in China in the country, and data localisation for network operators will be enforced from December 2018.

EGYPT

Telecommunications providers are restricted from sending some types of customer data across borders.

INDIA

Telecommunications licences contain provisions on the transfer of some types of customer data across borders.

INDONESIA

All electronic systems operators providing a public service (services provided by non-government institutions in areas like banking, insurance, health, security, industrial services and social activities) to set up a data centre and disaster recovery centre in Indonesian territory for the purpose of law enforcement and data protection.

HONG KONG

Recently published guidance to businesses exporting personal data which expressly prohibits the transfer of personal data to places outside Hong Kong except in circumstances specified in the Personal Data Ordinance.

VIETNAM

A decree issued in 2013 requires companies providing services across mobile networks, social networks, games services and all organisations with 'general websites' to have a minimum of one server inside Vietnam containing all information processed on the website or social network during at least the previous two years.



Regional Approaches Drive Consistency

**Regional initiatives (e.g., APEC CBPR and EU BCR)
build regulatory capacity in data privacy
and in the storage and movement of data**

Regional data privacy initiatives should be:

Streamlined and user-friendly

... to encourage applicants and uptake

Promoted to other regions

... spreading consistent rules based on common principles

Inter-operable

... enabling inter-region alignment and efficiencies



Laws, Governments and Regulators

Industry and business need the freedom to figure out what works best.

Being too prescriptive in regulation and enforcement can get in the way of the best outcomes for consumers.

Smart privacy regulation for consumers is:





Obrigado!

**Philippe Moura
Regulatory Manager**