GSMA Capacity Building

Principles of Mobile Privacy

Introduction

- With the rapid expansion of ICT, the law has sought to address, and keep pace with, the privacy and data protection challenges that new technologies and data processing capabilities bring about
- It is also becoming clearer that new technologies and ways to analyse data can help drive innovation, deliver significant social and economic benefits and meet pressing public policy needs
- ‘Data protection’ and ‘privacy’ are currently regulated by a patchwork of international and regional instruments, as well as by national and sectoral laws
- A key question is what is the most effective regulatory framework to use in order to secure these benefits, while protecting privacy — especially in a connected and increasingly converged world?
- What is the role of data protection and privacy in creating trust among consumers and citizens?
- What is the role of trust in economic growth and development?

Aims of this course

Distinguish between and understand key elements of ‘Privacy’, ‘Data Protection’ and ‘Security’ in the context of mobile & ‘connected’ devices

a. What is the role of these concepts in building consumers’ trust?

Highlight key privacy challenges – for service providers and regulators

a. Practical challenges
b. Policy and regulatory challenges / implications

Highlight key opportunities arising from data-driven innovation – Big Data

a. The role of regulation

How to future-proof privacy in regulation and policy

a. International privacy frameworks
b. Industry best practice

Outline of the Sessions

- Session1. Background – privacy and data protection
  - History, development and key concepts
- Session 2. Security
- Session 3. Privacy: The mobile internet context
- Session 4. Privacy in the Internet of Things (IoT) and Big Data
- Session 5. Future-proofing privacy in regulation and policy
- Session 6. Guided case study – Applying ‘Privacy by Design’
- Wrap Up

Capacity Building

SESSION 1

1 Background

- Privacy and data protection: History, developments and key concepts

Privacy is a key component of Trust in a ‘connected’ world

- Privacy
- Security

TRUST

- Accountability
- Usability

GSMA Research: Consumers' attitudes towards their privacy

- Insights from consumer research – attitudes towards their privacy

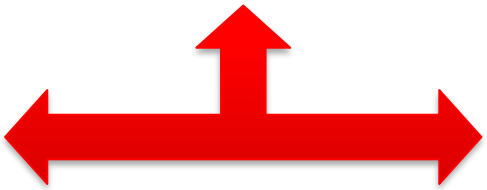
Privacy: what does it mean to you?

Do Not Disturb

70%

Of mobile users would like to set their preferences for the types of as they receive on their mobile and when

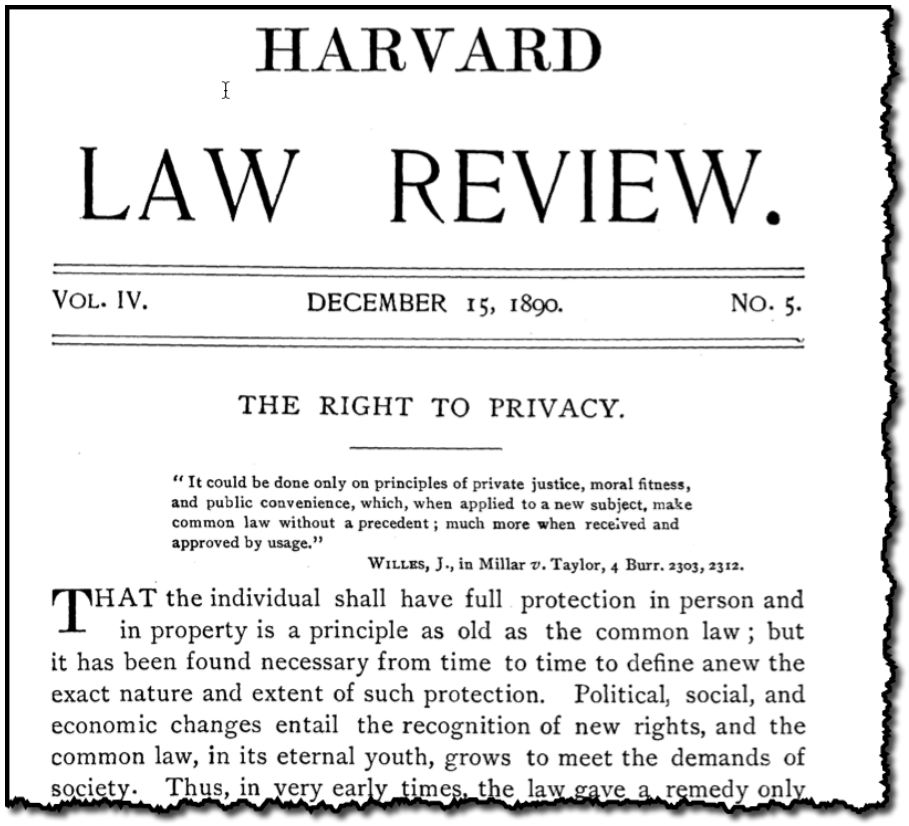
Privacy



Secrecy
Anonymity
Freedom of movement and association
Safety
Solitude

Control
Fundamental right
Dignity
Intimacy

Privacy as a concept — it is not new



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only

A right to privacy?

- UN – Universal Declaration of Human Rights 1948 (Article 12: The right to the protection of an individual against intrusion into their private sphere)
- UN - International Covenant on Civil and Political Rights (Article 17: 1 - No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2 - Everyone has the right to the protection of the law against such interference or attacks.)
- European Convention on Human Rights: right to respect for family and private life (Article 8) – “Everyone has the right to respect for his private and family life, his home and his correspondence”
- EU Charter of Fundamental Rights:
  - respect for private and family life (Article 7) - “Everyone has the right to respect for his or her private and family life, home and correspondence” and
  - protection of personal data (Article 8) – “Everyone has the right to the protection of personal data concerning him or her”
- US – The Fourth Amendment to the U.S. Constitution establishes the right to be secure against unreasonable searches and seizures. While this does not expressly reference a right to privacy, it has established law related to reasonable expectations of privacy with regard to government access.

Aspects of online and mobile privacy

Informational privacy

Communications privacy

Spatial privacy **(location and context)**

Privacy – the link to data protection

EU Charter of Fundamental Rights:

Protection of personal data (Article 8)

"Everyone has the right to the protection of personal data concerning him or her.

*Such data must be processed **fairly** for **specified purposes** and on the basis of the **consent** of the person concerned or some other **legitimate basis** laid down by law*

*Everyone has the **right of access** to data which has been collected concerning him or her, and the right to have it **rectified.**"*

Data protection law — developments

Today, there are approximately 120 data protection and privacy laws which have been influenced by a few reports, guidelines, conventions, directives and regulations

2018

1973

US: Fair Information Practices (1973)

OECD Privacy Guidelines (1980)

Council of Europe Convention 108 (1980)

EU Data Protection Directive 95/46 (1995)

APEC Privacy Framework (2005)

EU General Data Protection Regulation (2018)

Data Protection Law — the basics

A data protection law in a specific country generally:

- Places obligations and restrictions on collection and and use of ‘personal data’
- Could be ‘Omnibus’ OR sector specific
- Gives rights to individuals
- Defines key concepts:
  - **Personal data**
  - **Data Processing**
  - **Data Controller**
  - **Data Processor**
  - **Data subject**
  - **Consent**
- …And sets out key privacy principles

Data Protection Law - KEY principles

- Process data fairly and lawfully
- Process data only for specified purposes
- Collect and use the minimum amount of data necessary
- Keep data accurate and up-to-date
- Keep data only as long as necessary
- Respect the rights of individuals
- Keep data secure (via technical and organisational means)
- Ensure adequate accountability if sending data overseas

What is ‘Personal data’?

Data protections laws only apply to **personal data** (e.g., data that can be used to identify a living individual or that relates to an identifiable individual)

Examples?

Data protection law also covers sensitive personal data

What is ‘consent’?

Consent is a cornerstone of data protection law and one of a number of legal conditions for process personal data.

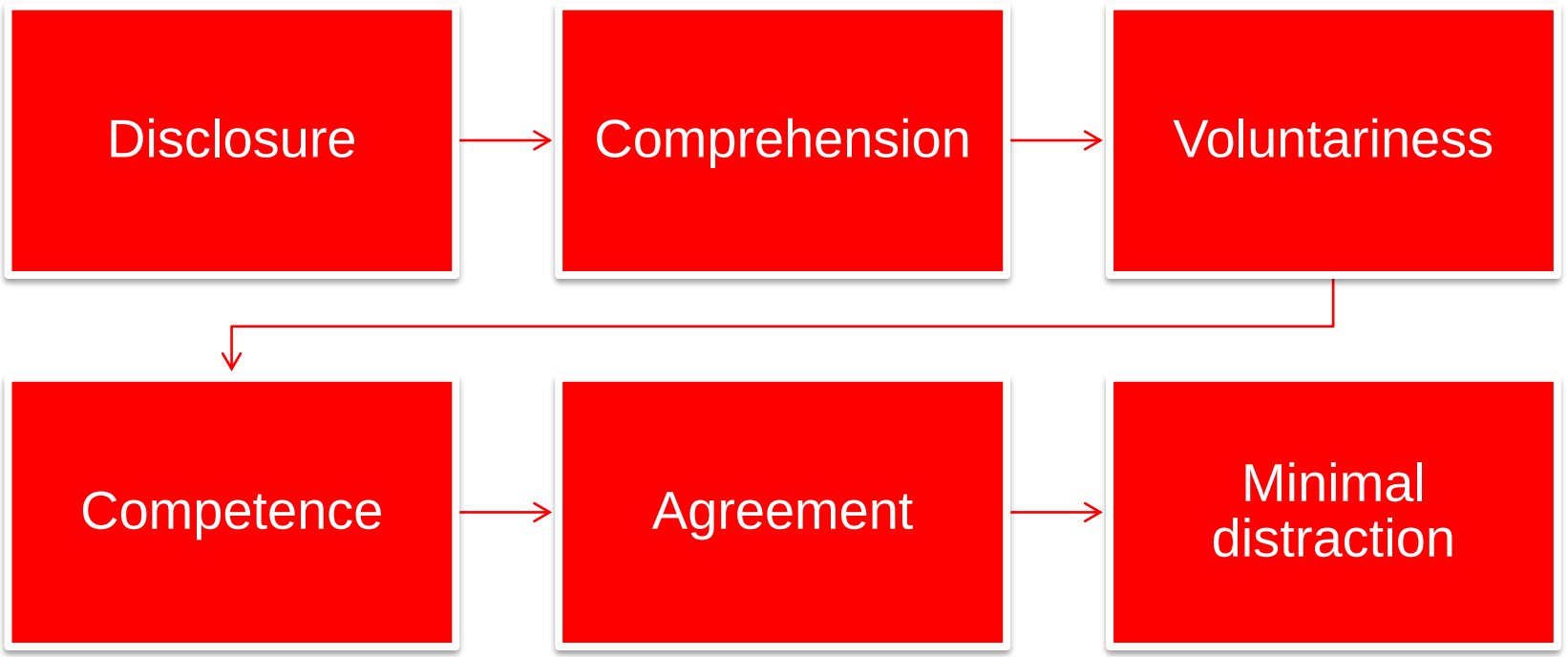
Under the current EU Directive 95/46EC, consent means: *"any freely given specific and informed indication …. by which the data subject signifies his agreement to personal data relating to him being processed*" (explicit consent is required for ‘sensitive data’)

Under the AU Convention, it means: *“any manifestation of express, unequivocal, free, specific and informed will by which the data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing”*

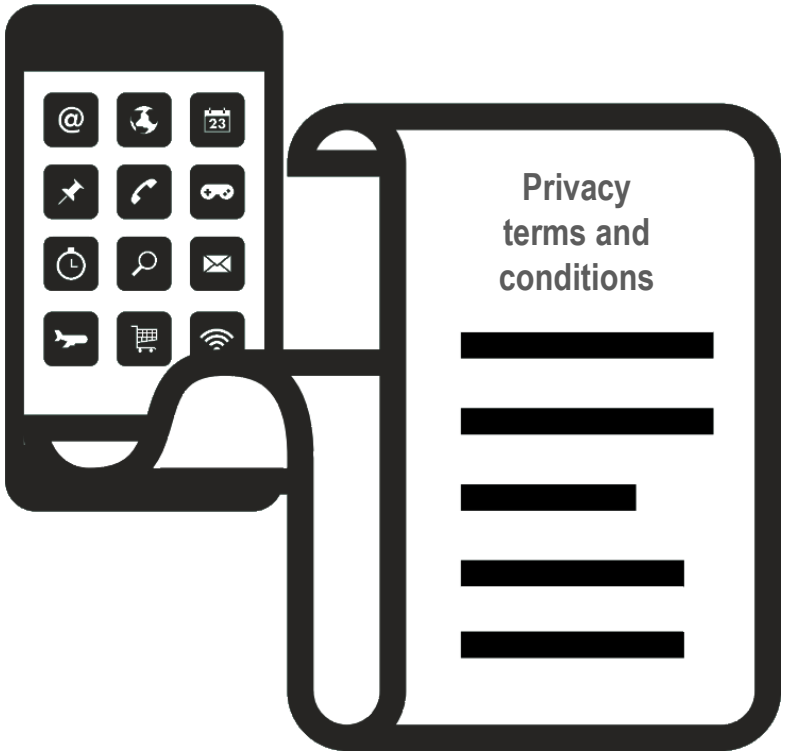
Under the EU General Data Protection Regulation, which comes fully into effect in May 2018, consent should be given by: *“a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.”*

Key elements of consent

Designing for (informed) consent and user trust:



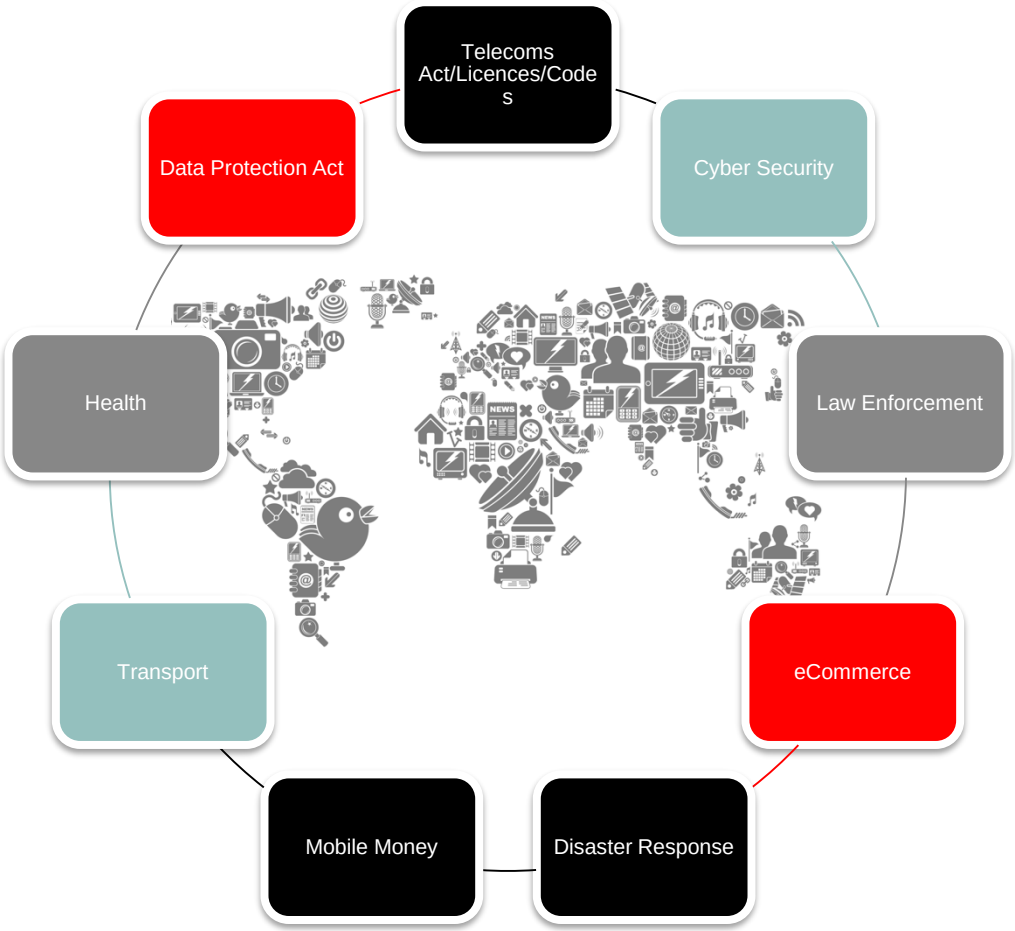
Users agree privacy policies without reading them — what does this mean?



80%

of mobile internet users who ‘agree’ to privacy policies without reading them said it is because they are “too long”

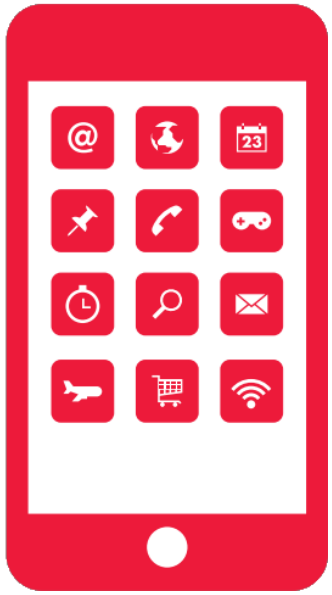
Data 'protection' — varies by region and sector



Most mobile internet users are concerned about sharing personal information

83%

of mobile internet users have concerns about sharing their personal information when accessing the internet or apps from a mobile



Base: All mobile internet users

Telecommunications privacy

Key objectives of privacy regulations as they apply to telecommunications companies:

- Confidentiality of communications
- Protection against unauthorised monitoring or surveillance
- Security of communications, networks *and* data
- Privacy of traffic, location and billing data
- Rights for callers to present or withhold calling the identity
- Restrictions on marketing and secondary data use

But what if an internet/IP service is not provided by a telecommunications player?

Telecommunications laws: privacy asymmetries

In addition to general data protection and privacy laws, mobile and fixed operators are also subject to additional obligations related to the processing of data

- License conditions
- Multimedia/communications laws
- E-Privacy laws
- Interception and disclosure laws (for law enforcement purposes)
- Data retention laws
- Electronic transactions laws
- Statutory codes of conduct, or guidelines

What does this mean for consumers who may be using equivalent services provided by non-telecommunications providers?

Capacity Building

1

SESSION 1

Recap

- What do we mean by privacy and data protection?

Capacity Building

SESSION 2

2 Security

Security is a key component of Trust in a ‘connected’ world

- Privacy
- Security

TRUST

- Accountability
- Usability

Security is NOT the same as privacy

≠

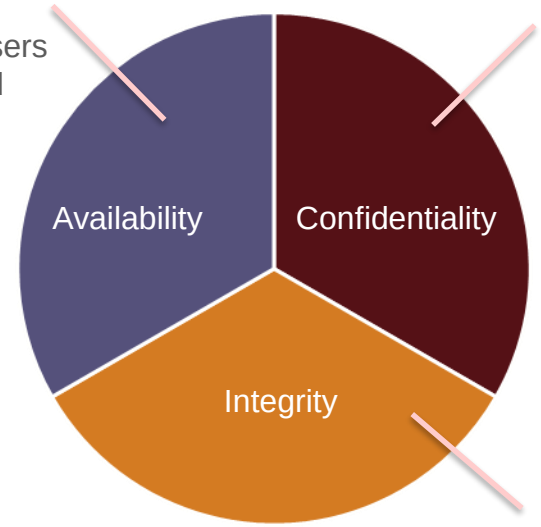
Requirements ensuring security and integrity of networks and services

Providers of public communications networks, or publicly available electronic communications services, are required to take:

- Technical and organisational measures to reduce and manage risk
- All appropriate steps' to guarantee integrity of networks and minimise the risk of data breaches
- Act and report personal data breaches

Mobile security objectives — an element of data protection law

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability



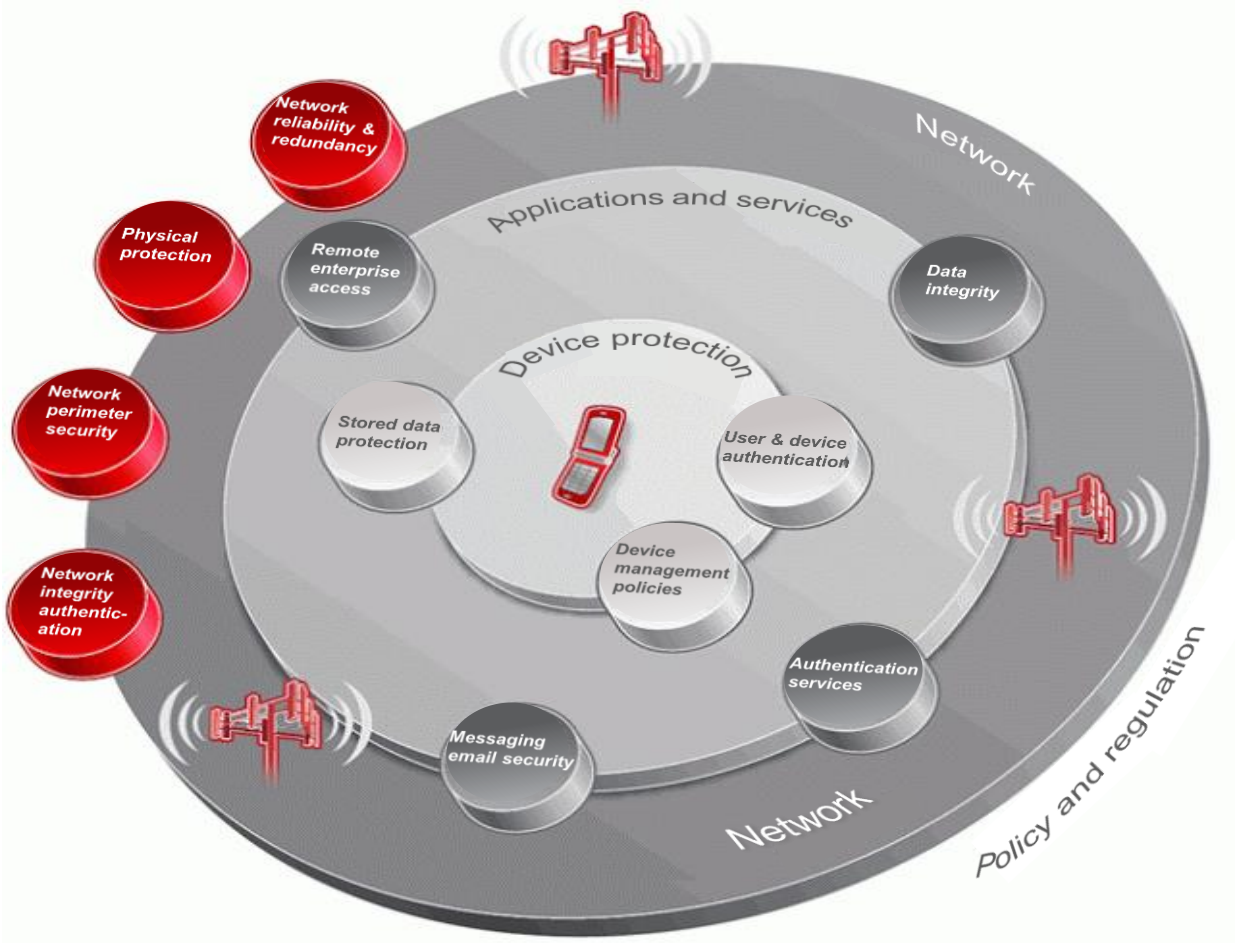
Assures that information systems – and data contained in them – are available to authorised users when needed

Assures that information is disclosed only to authorised individuals and systems

Guards against improper information modification or destruction

Source: Mitre

Key elements of mobile security management



Capacity Building

2

Session 2: Security

Group Discussion

- Recap of what we've covered so far
- What experiences can you share from your individual countries?
- What do you see as the key privacy and data protection challenges?

Capacity Building

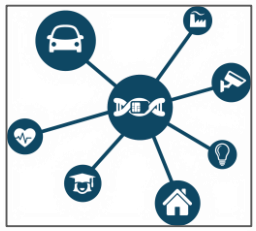
3

Session 3

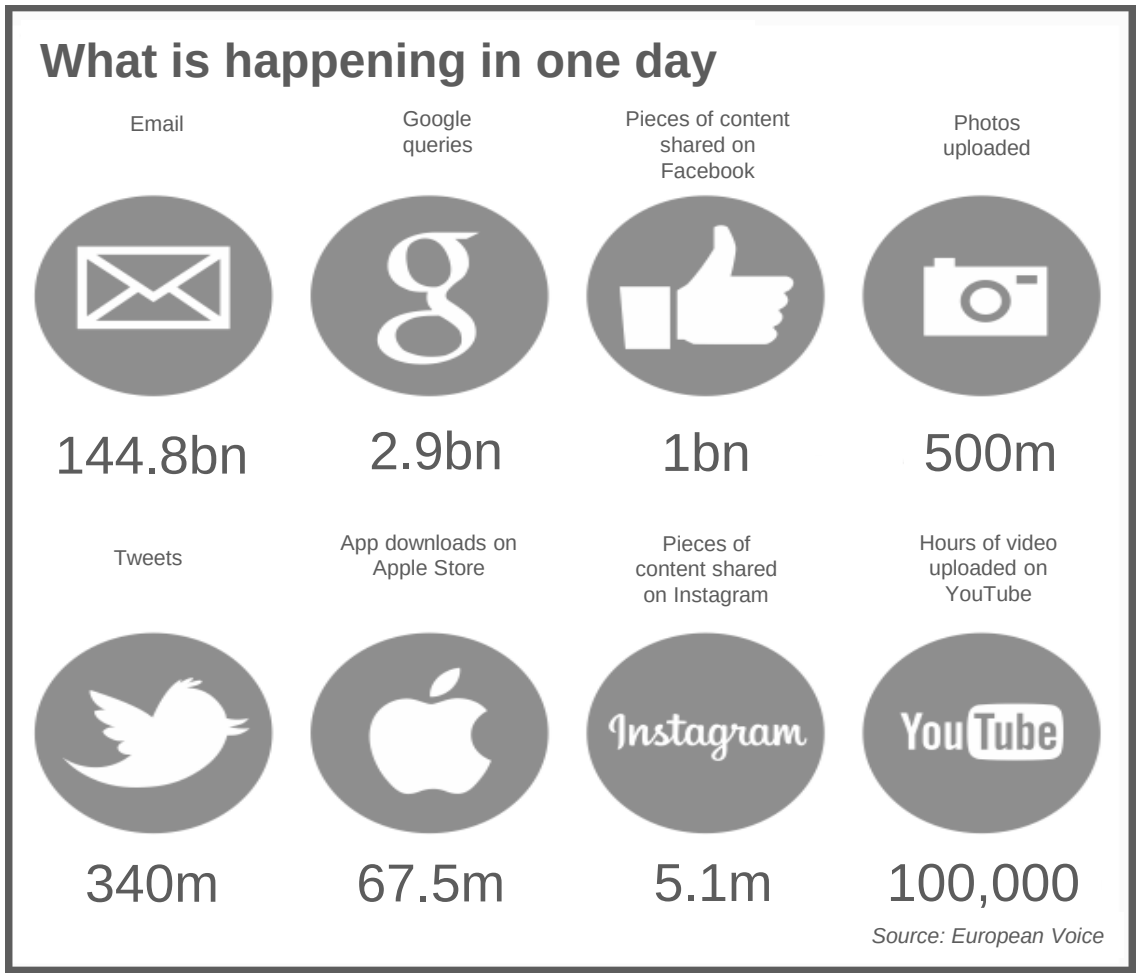
Privacy: The mobile internet context

The modern smartphone

- A smartphone now has computing power superior to the computers needed to send a man to the moon in 1969

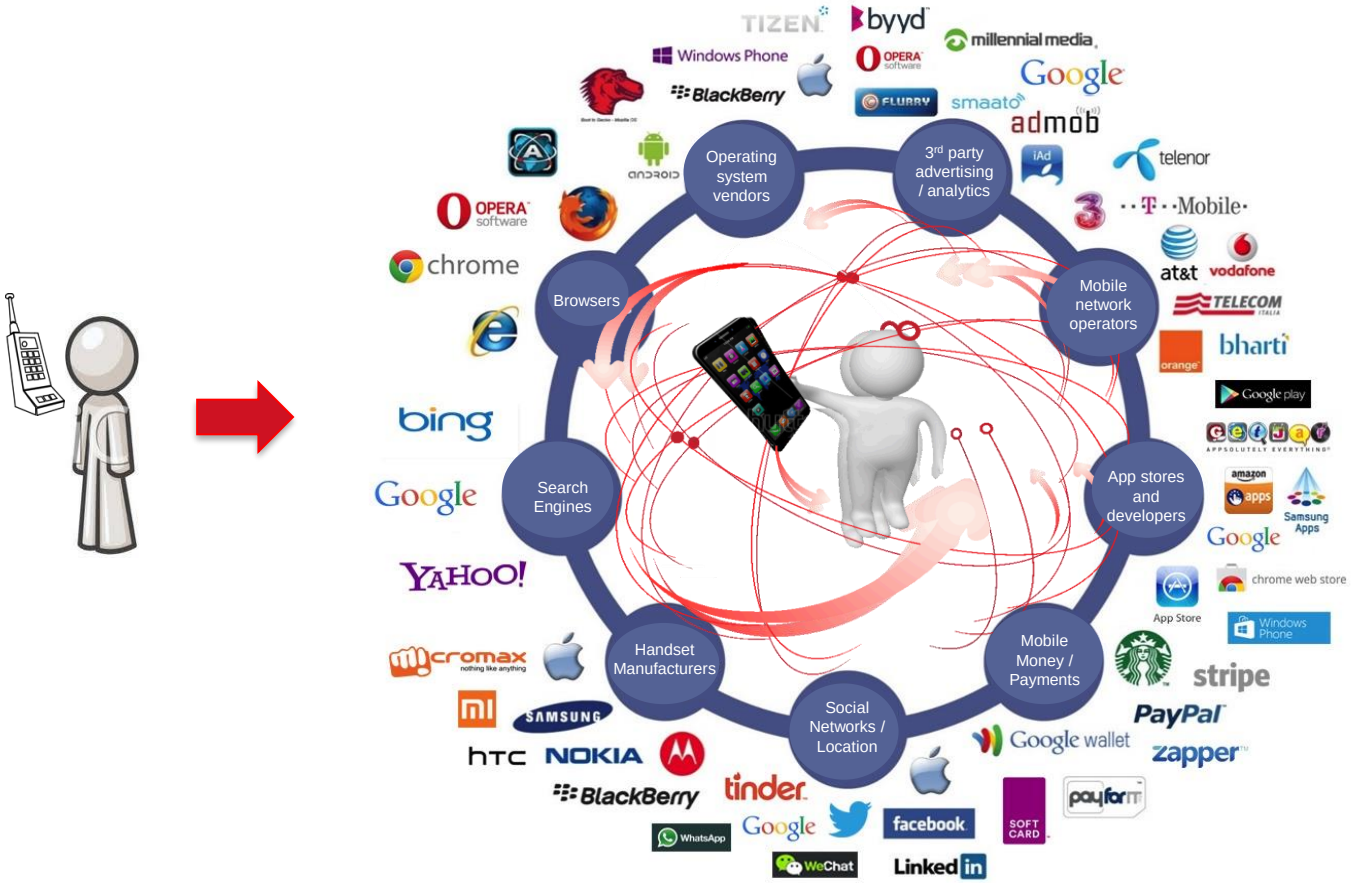


A day in the life of the internet

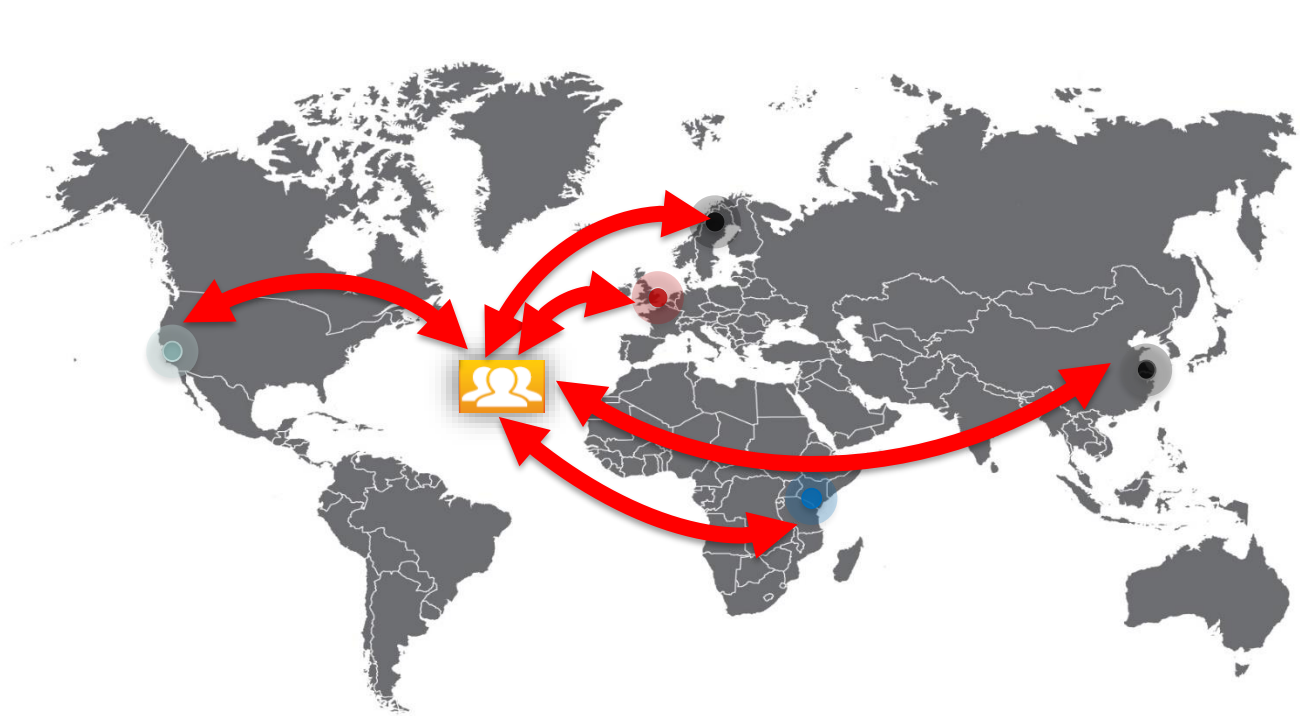


Source: http://blog.digital.telefonica.com/wp-content/uploads/2014/06/Data-the-new-currency.pdf

A day in the life of the internet (cont'd)



Mobile privacy context: Data flows globally and accessed by multiple parties



User

App Store

Mobile operator

Mobile analytics company

Device manufacturer

App developer

How would converging services impact privacy policy and regulation?

- Instant messaging and VoIP are offering services equivalent to traditional communications

- But laws differ, so how can policymakers offer:

  - Legal certainty and level playing field for business?
  - Consistency in privacy experiences of users?
  - Innovation that drives public policy objectives?

Location data and privacy

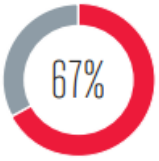
- Where I am now + activity/context?
- Where I am not (normally)?
- Where I am heading?
- Where I have been?
- Which route have I travelled?
- Which way I am facing / what is my elevation?
- What people and things I am connected to?

Location data and privacy

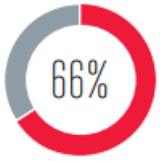
Location and traffic data: inconsistencies in regulation affecting consumers …

60%

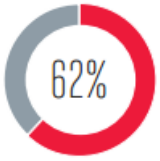
of mobile users want a consistent set of rules to apply to any company accessing their location, regardless of how they obtain this information



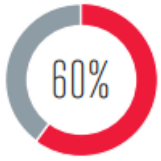
UK



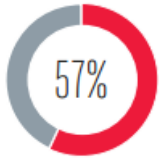
Colombia



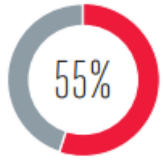
Mexico



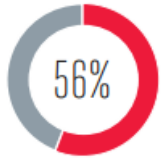
Indonesia



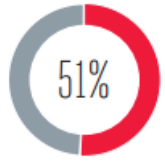
Singapore



Brazil



Malaysia



Spain

Location and traffic data: inconsistencies in regulation affecting businesses…

GPS location
(limited or no regulation)

WiFi location
(limited or no regulation)

Cellular location
(highly regulated)

Capacity Building

3

Session 3: Privacy – the mobile internet context

Group Discussion

1. What do we mean by privacy and data protection? How is this complicated by location data?
2. What do you see as the key privacy and data protection challenges?

Capacity Building

Session 4

4

Privacy in the Internet of Things (IoT) and Big Data

What do we mean by the ‘IoT’?

A world in which consumers and businesses enjoy rich new services, connected by intelligent and secure mobile network

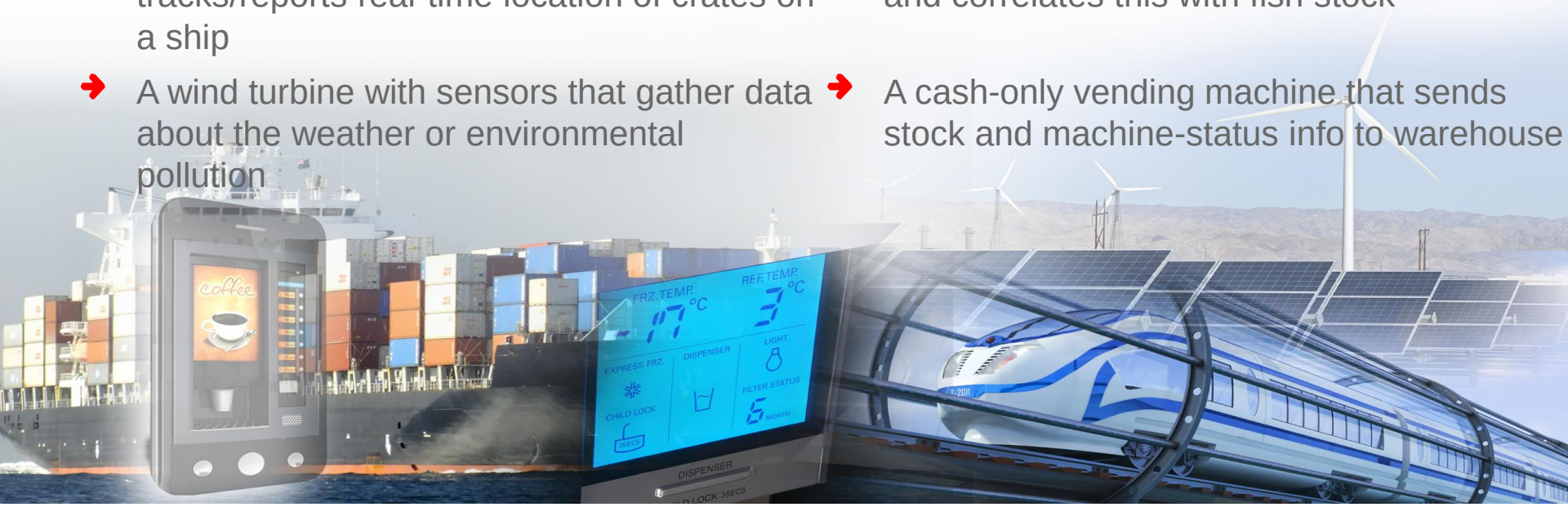
The IoT will involve more connected sensors and devices creating and collecting data in real time…

- Accessed or shared by a potentially unlimited number of companies
- Better data = more insights

While the IoT will create more data and insights… not all will be about consumers

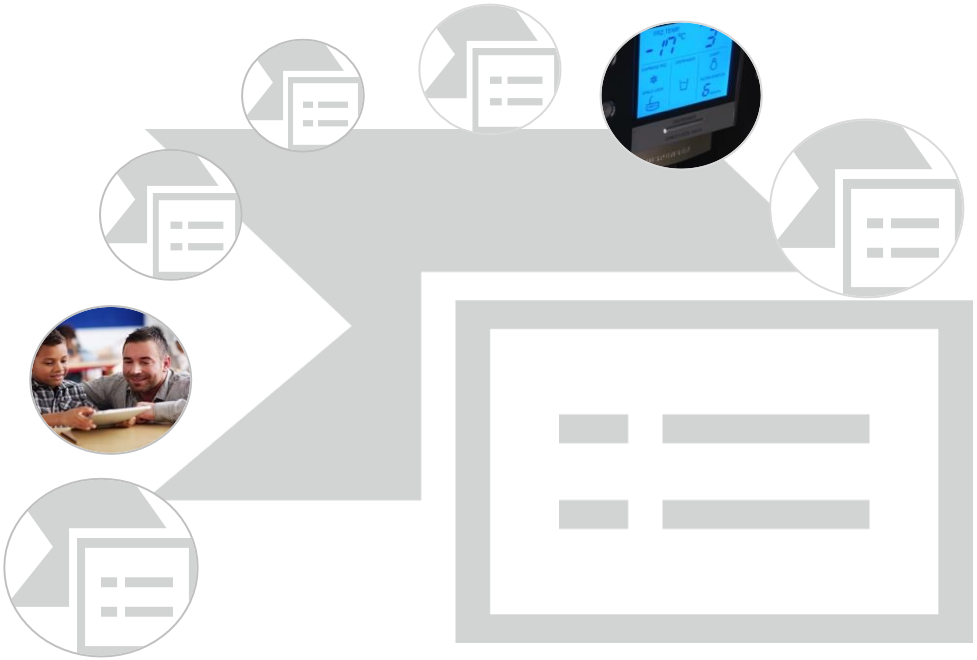
‘Purely industrial’ IoT services are unlikely to impact consumers’ privacy e.g.

- A cargo monitoring company that tracks/reports real-time location of crates on a ship
- A wind turbine with sensors that gather data about the weather or environmental pollution
- A fish farm that monitors water temperature and correlates this with fish stock
- A cash-only vending machine that sends stock and machine-status info to warehouse



Consumer ‘IoT’ devices and privacy

- Many IoT services can directly improve people’s lives …



….But can also lead to negative consequences…

Existing privacy rules are adequate for IoT if applied in a technology-neutral way

- IoT involves many parties from both the private and public sector
- Effective privacy protection requires existing rules to apply consistently across all IoT providers in a service and technology-neutral way…
- …but privacy and security practices should reflect the overall risk of harm to an individual in a given context
- Governments and regulators can unlock a range of socio-economic benefits from IoT by interpreting existing frameworks more flexibly or implementing policies that
  - promote innovation and investment
  - meet consumers' expectations and build their confidence and trust
  - apply existing data protection principles in a technology neutral way

Big Data — what is it?

The exponential growth both in the availability and automated use of information

References to Big Data generally involve:

- **Large** data quantities from **multiple and diverse** data sources (volume, variety)
- Created in **near-real time**, (velocity)
- The use of **data processing** techniques to analyse the data, **identify correlations and generate** (potentially unexpected) **insights** that might have a predictive quality

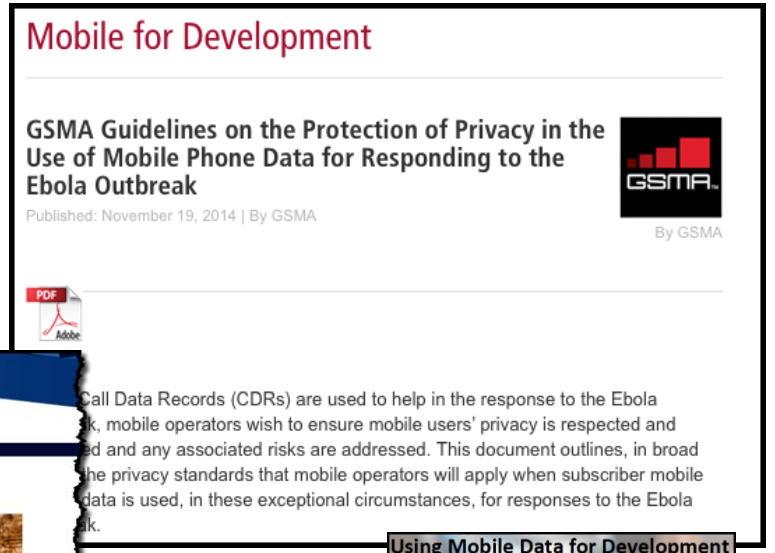
Big Data — what can it do?

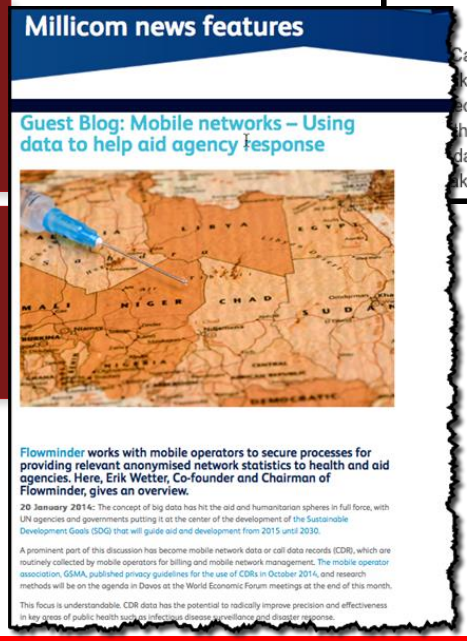
Potential areas of use

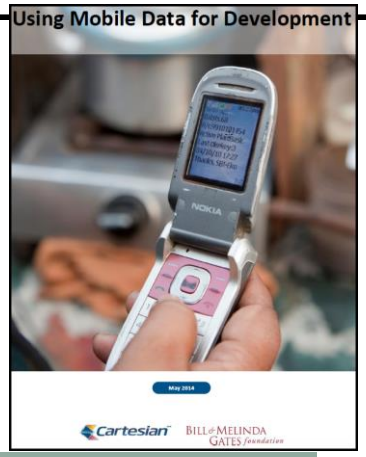
Predicting the spread of infectious disease

Optimising urban planning and management

Open data innovation — creating opportunities







Regulatory considerations for advancing Big Data opportunities (Data Innovation Vs Data Protection)

Could over-regulation on user privacy destroy both private value and public good – what is the right balance?

Key regulatory considerations:

- How can policymakers facilitate the use of Big Data by governments in order to meet pressing public policy needs?
- How strict should rules be in relation to companies 'specifying' the uses of personal data, given that Big Data may well lead to predicting future 'undiscovered' uses?
- How can consumer 'notice' and 'consent' rules be applied in the context of Big Data without inhibiting innovation? (e.g. when new data uses are conceived after collection)
- How can policymakers facilitate cross-border data transfers while ensuring consumers' privacy is respected? (e.g. through privacy protective methods)
- Who controls one's data when smart devices process data without human intervention to make market predictions?

Capacity Building

4

Session 4: Big Data

Activity 1

1. Do any of you have experience of Big Data in your everyday lives?
2. What do you think are the key challenges related to Big Data?
3. How would you address these challenges?
4. To what degree should society have a say in Big Data policy?

Capacity Building

4

Session 4: Big Data

Activity 2

1. We often hear that ‘trust’ is important to consumers and citizens.
2. What does trust mean to you?
3. What do you believe are the key elements of trust?
4. Is there evidence from your own country that trust matters?

Capacity Building

5

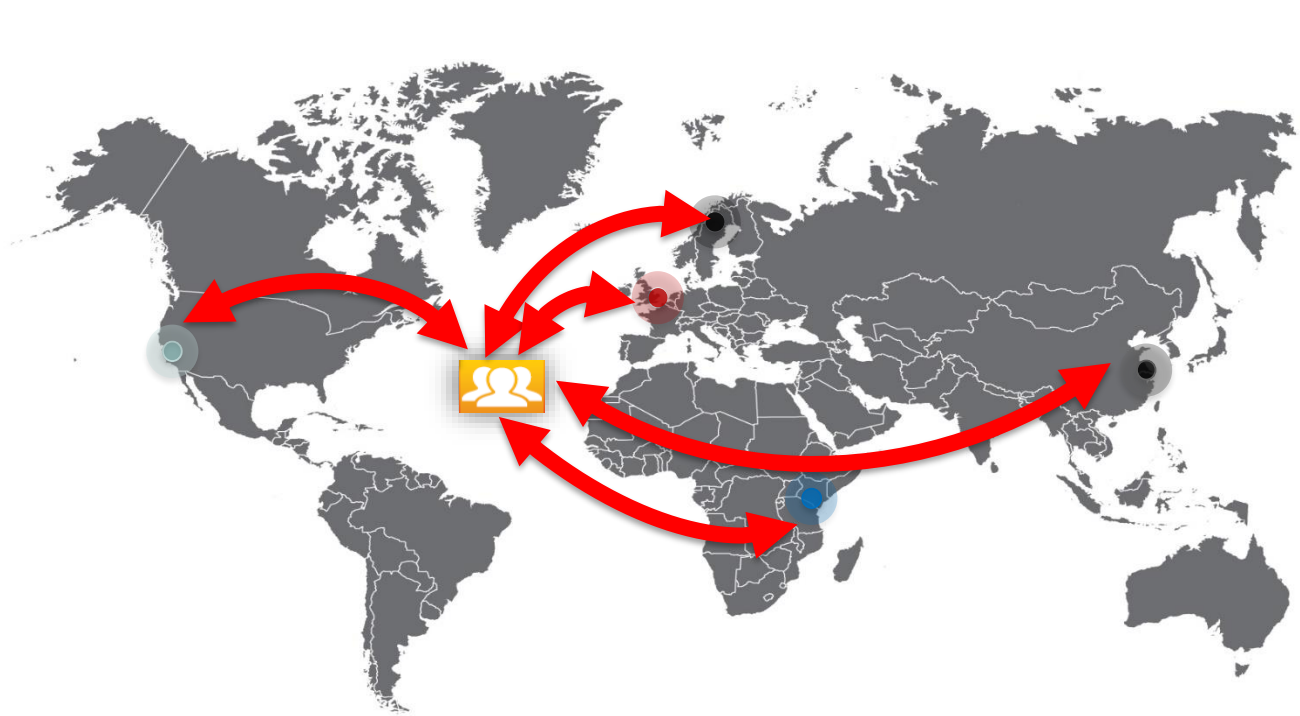
SESSION 5

Future-proofing privacy in regulation and policy

Remember…


Operating system vendors
3rd party advertising / analytics
Mobile network operators
App stores and developers
Mobile Money / Payments
Social Networks / Location
Handset Manufacturers
Search Engines
Browsers
TIZEN
byyd
millennial media
Windows Phone
BlackBerry
OPERA software
FLURRY
smaato
Google
admob
android
iAd
telenor
T-Mobile
at&t
vodafone
TELECOM ITALIA
orange
bharti
Google play
chrome
OPERA software
bing
Google
YAHOO!
amazon apps
Samsung Apps
chrome web store
App Store
Windows Phone
stripe
PayPal
zapper
Google wallet
payforit
SOFT CARD
facebook
Linked in
WeChat
WhatsApp
tinder
BlackBerry
NOKIA
htc
SAMSUNG
mycromax

Mobile privacy context: Data flows globally and accessed by multiple parties



User

App Store

Mobile operator

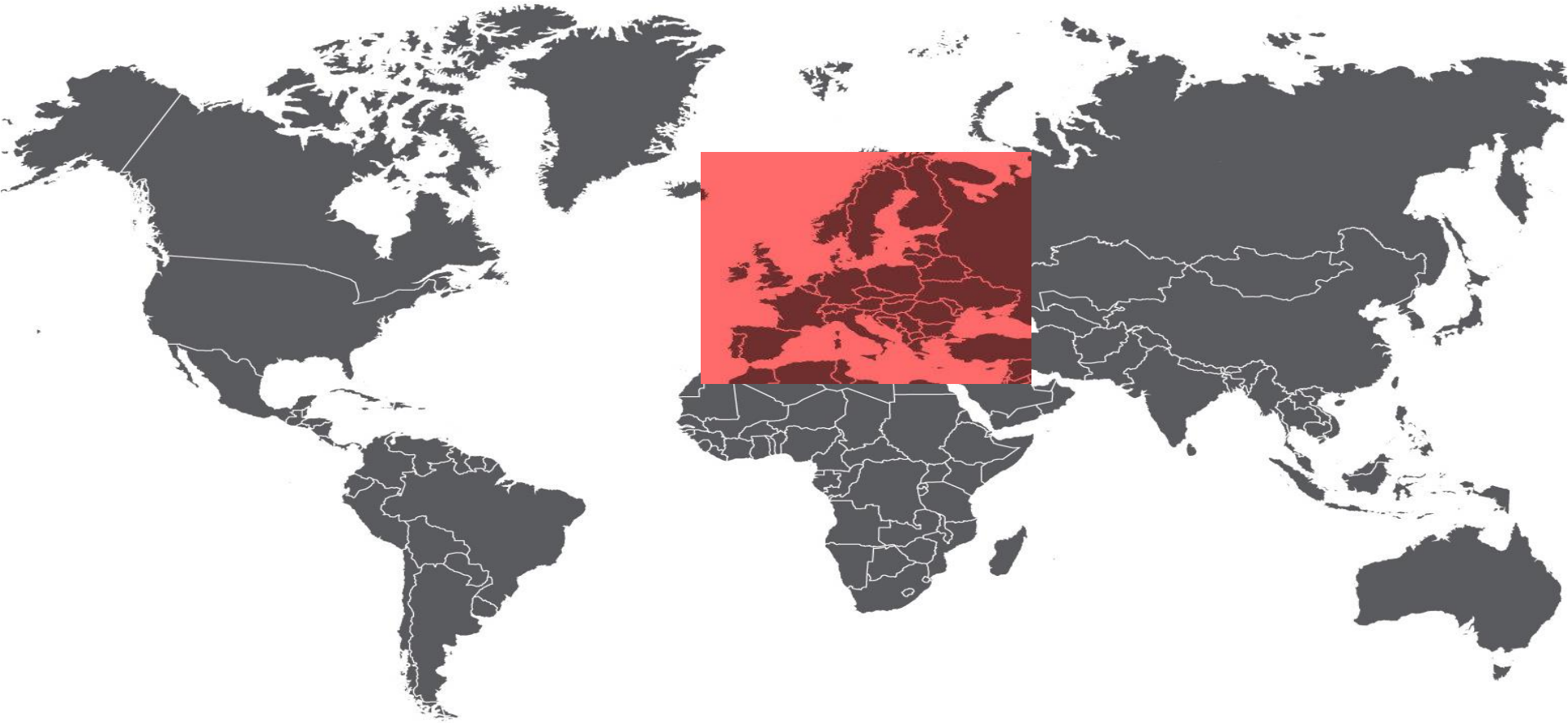
Mobile analytics company

Device manufacturer

App developer

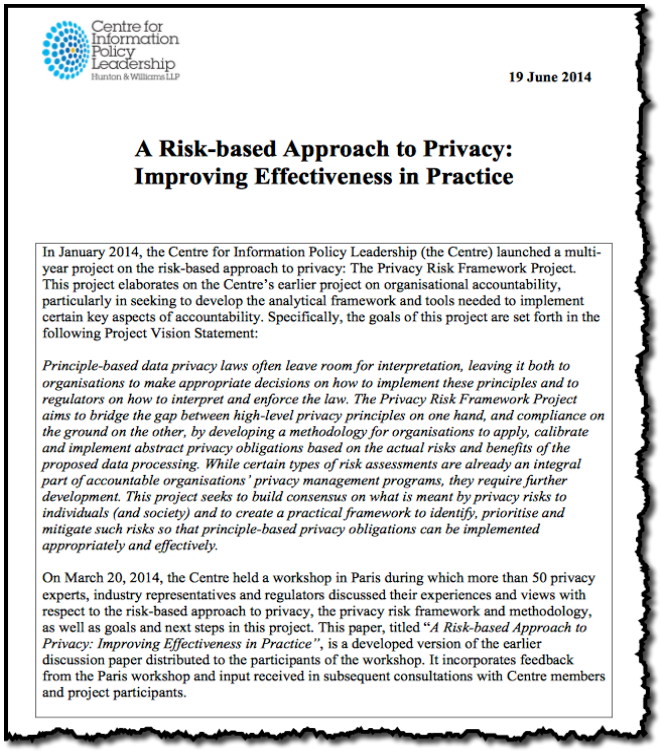
Policymakers across the world are rethinking privacy regulation

EU regulators lead the way towards strengthening data protection



The importance of a risk based approach when considering new privacy rules

Empowering the industry to identify and mitigate the risk in the specific context of developing a new service.



Centre for Information Policy Leadership
Hunton & Williams LLP

19 June 2014

A Risk-based Approach to Privacy: Improving Effectiveness in Practice

In January 2014, the Centre for Information Policy Leadership (the Centre) launched a multi-year project on the risk-based approach to privacy: The Privacy Risk Framework Project. This project elaborates on the Centre's earlier project on organisational accountability, particularly in seeking to develop the analytical framework and tools needed to implement certain key aspects of accountability. Specifically, the goals of this project are set forth in the following Project Vision Statement:

Principle-based data privacy laws often leave room for interpretation, leaving it both to organisations to make appropriate decisions on how to implement these principles and to regulators on how to interpret and enforce the law. The Privacy Risk Framework Project aims to bridge the gap between high-level privacy principles on one hand, and compliance on the ground on the other, by developing a methodology for organisations to apply, calibrate and implement abstract privacy obligations based on the actual risks and benefits of the proposed data processing. While certain types of risk assessments are already an integral part of accountable organisations' privacy management programs, they require further development. This project seeks to build consensus on what is meant by privacy risks to individuals (and society) and to create a practical framework to identify, prioritise and mitigate such risks so that principle-based privacy obligations can be implemented appropriately and effectively.

On March 20, 2014, the Centre held a workshop in Paris during which more than 50 privacy experts, industry representatives and regulators discussed their experiences and views with respect to the risk-based approach to privacy, the privacy risk framework and methodology, as well as goals and next steps in this project. This paper, titled "*A Risk-based Approach to Privacy: Improving Effectiveness in Practice*", is a developed version of the earlier discussion paper distributed to the participants of the workshop. It incorporates feedback from the Paris workshop and input received in subsequent consultations with Centre members and project participants.

- Data protection/privacy impact assessments can be used as a tool to evaluate and mitigate privacy risks.
- Evaluating privacy risks during the initial phases of product development can help build privacy controls into the product and reduce risk to individual privacy.
- Data protection impact assessments will be required prior to 'high risk' data processing under Article 35 of the new EU General Data Protection Regulation.

Increasing international regulatory co-operation and enforcement

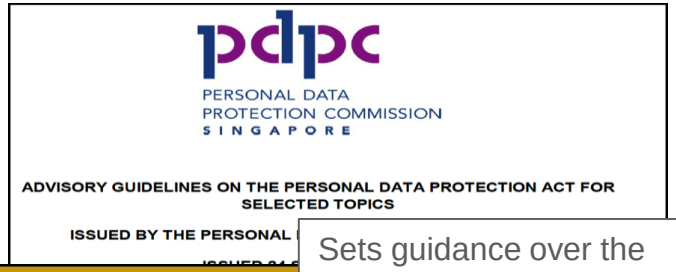
Global Privacy Enforcement Network

FAPDP
Forum Africain sur la Protection des Données Personnelles
FA/PDP - DAKAR 2015

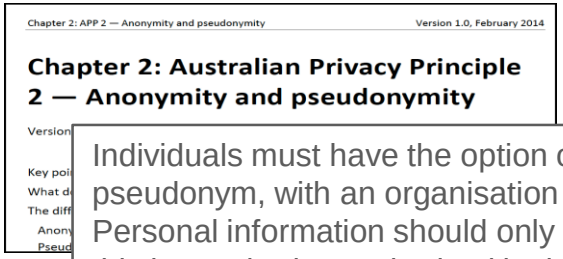
RED IBEROAMERICANA DE PROTECCION DE DATOS

ASSOCIATION FRANCOPHONE DES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES

Increased regulatory efforts to promote data *anonymisation & pseudonymisation*



Sets guidance over the anonymisation and pseudonymisation of personal data.



Individuals must have the option of dealing anonymously, or by pseudonym, with an organisation (subject to an exemption). Personal information should only be linked to a pseudonym if this is required or authorised by law, it is impracticable for the entity to act differently, or the individual has consented to providing or linking the additional personal information.

The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations.

- Irreversibly and effectively anonymised data is not “personal data”…
- If the source data is not deleted at the same time that the anonymised data is prepared, the anonymised data will still be considered “personal data”…

Right to Privacy – Global stage

Special UN Rapporteur for the Right to Privacy

United Nations A/HRC/28/L.27

General Assembly

Distr.: Limited
24 March 2015

Original: English

Human Rights Council
Twenty-eighth session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Industry initiatives – addressing privacy, beyond legal compliance

The GSMA's mobile privacy principles

1 — Openness, transparency and notice

2 — Purpose and use

3 — User choice and control

4 — Data minimisation and retention

5 — Respect user rights

6 — Security

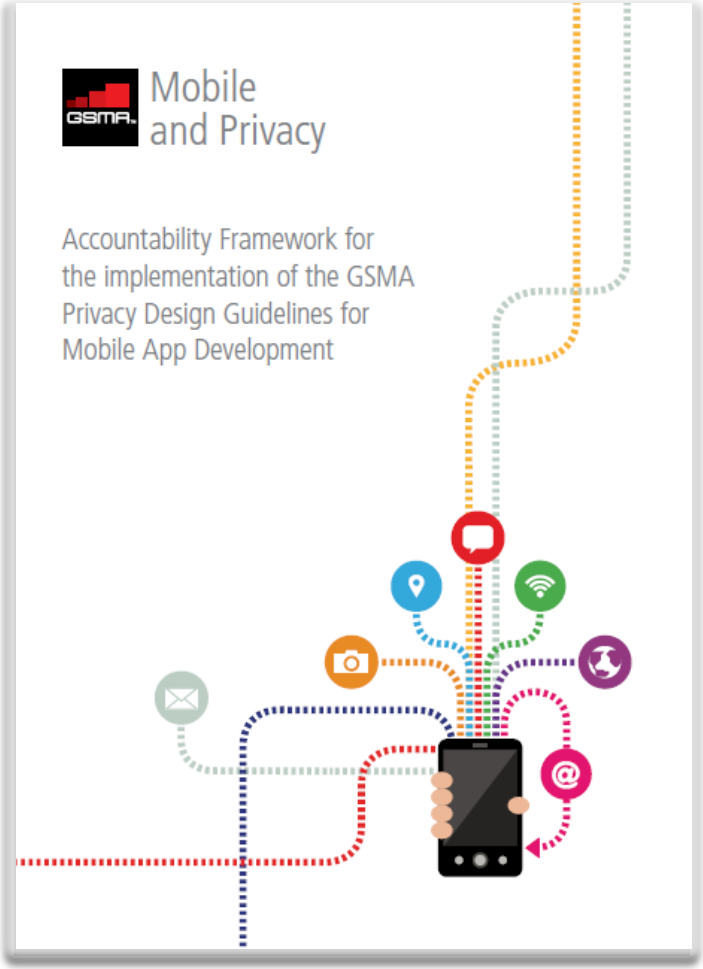
7 — Education

8 — Children and adolescents

9 — Accountability and enforcement

GSMA ‘privacy by design’ app guidelines – applying the principles in practice

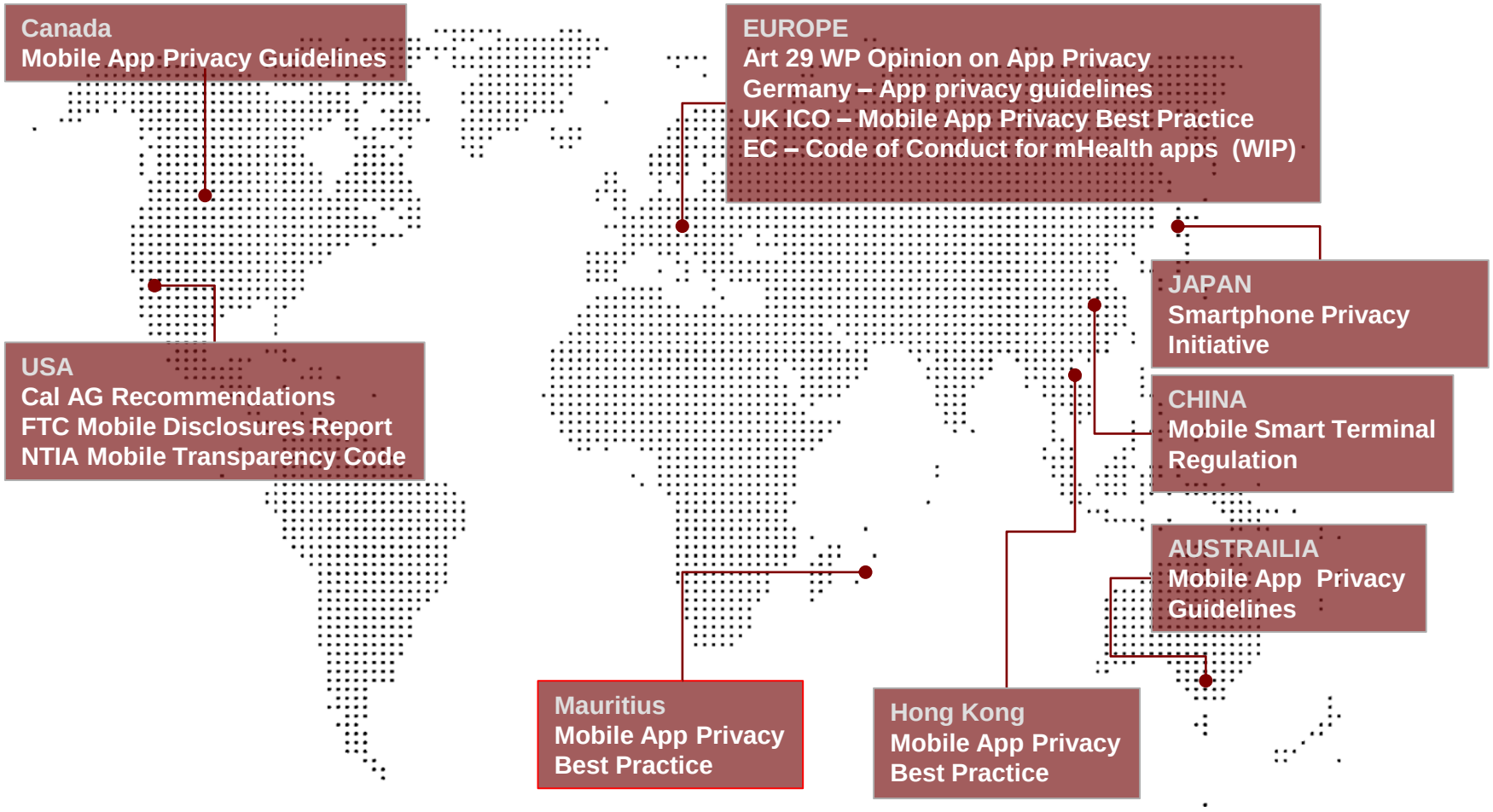
Accountability



'**Accountability**' is found in both the OECD guidelines and APEC privacy framework, and is also proposed in the draft EU General Data Protection Regulation.

In the context of the GSMA initiative, accountability is the acceptance and demonstration of compliance with commitments — "say what you do, and do what you say".

Mobile App Privacy – Regulatory Action



Group discussion: Deep dive on the principle of Transparency

What is it about?

- Being honest and open with consumers
- Helping consumers make informed decisions
- Should be proportionate to the level of risk

How can companies be transparent with consumers in practice?

- Simplified notices, just-in time notices, privacy icons and dashboards (to provide users with the means to set preferences)
- Feedback and awareness tools (such as interactive ‘touch points’) that highlight privacy-relevant activities around the use of a service

In short:
Tell users who you are, what personal information you require, what you intend to do with it and who you intend to share it with (and why!) — but don’t overburden them with prompts

Group discussion: Giving consumers choice and control over their privacy

Consumers want to be able to make choices about how their data is used. How can service providers help users manage their privacy?

- Tell them what the privacy default settings are and how to change them
- Clarify what (additional) personal information needs to be collected in order for a particular (optional) feature of the service to function
- Provide simple choices and mechanisms so users can express their privacy preferences. For example, allow them to decide
  - whether they want to share their email address in order to receive relevant offers
  - whether they want the service to 'remember' their log-on credentials, billing address, location etc.
  - How often they want to be prompted about their preferences

For more info see the GSMA's Privacy Design Guidelines for mobile app developers

Capacity Building

6

SESSION 6

Guided Case Study Scenario

- Is mobile privacy an issue in your country? What are the issues? What policy approaches are being considered?

Capacity Building

6

SESSION 6

Guided case study – Applying ‘Privacy by Design’

Capacity Building

6

SESSION 6

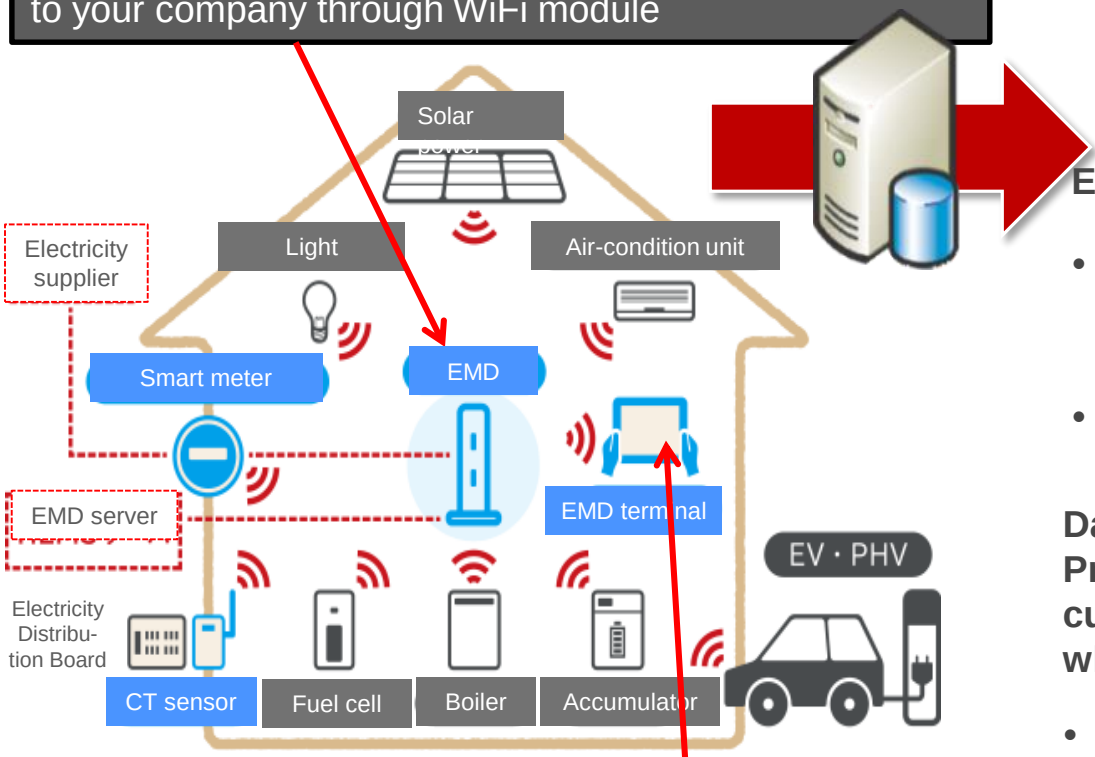
Guided Case Study

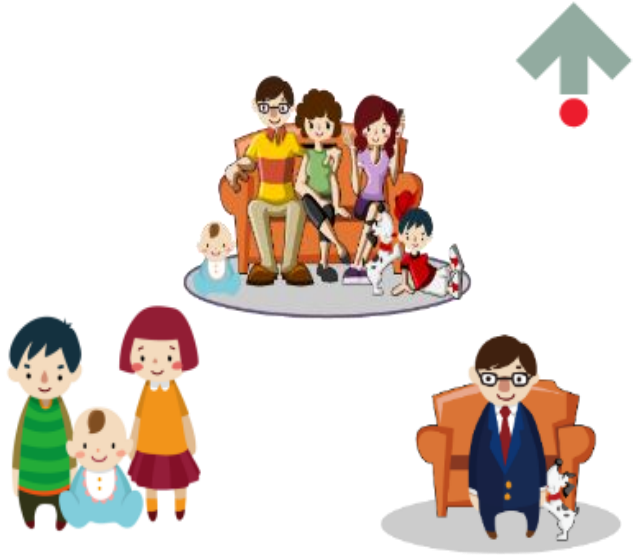
1. Read the service description on the next page (case study) about an Energy Management Device (EMD) and how consumers' data are to be used
2. Develop a recommended guide (Steps) that the service provider should take when developing their product (EMD) to ensure they properly consider the end user's privacy (Privacy by Design)

Capacity Building

Service description

1. Energy Management Device (EMD) installed at consumer's house and monitors energy consumption in each room. It's connected to the internet and sends data to your company through WiFi module





Energy usage information used to predict:

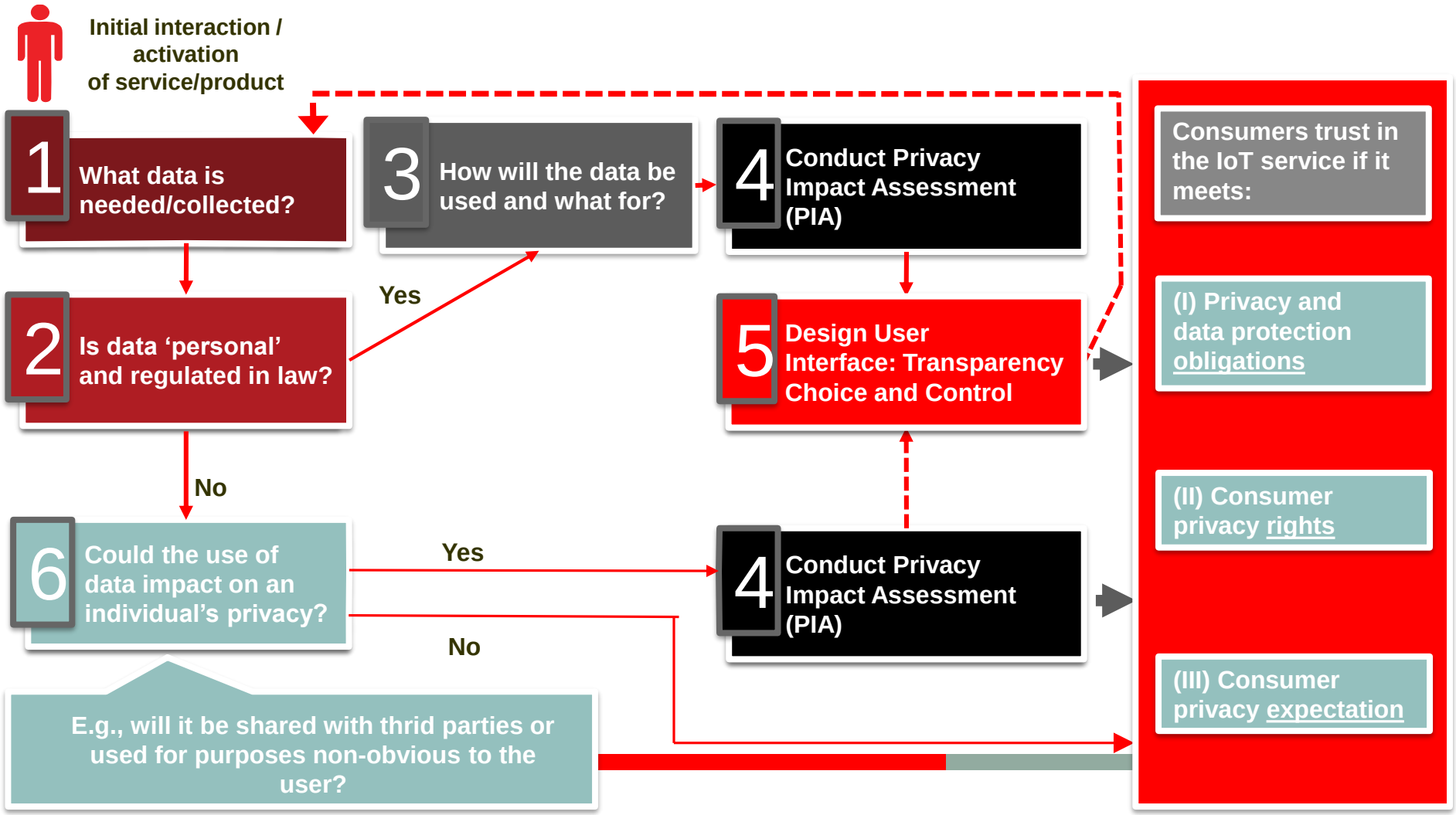
- User's 'lifecycle and lifestage' information (household type, whether retired or not, number of occupants, including children in the house etc.)
- User's lifestyle: information such as preferred services consumed (TV, video, music, shopping)

Data analysed to develop consumer insights - Predictions can be used to allocate customers to specific segments based on which targeted offers can be sent e.g.:

- Coupons for free / discounted services
- Video / entertainment services
- Other service recommendations

2. Consumers can monitor their energy consumption on a tablet through a dedicated app/web portal

Possible steps for IoT service providers to ensure Privacy by Design



Considerations: Assessing and mitigating risk

4 Conduct Privacy Impact Assessment (PIA)

Conducting a Privacy Impact Assessment (PIA) is about:

- Identifying and reducing the privacy risks of your project
- Reducing the risk of harm to individuals through the possible misuse of their personal information
- Designing a more efficient and effective process for handling data about individuals

Questions to help you assess the need for a PIA include:

- Will the project result in you/your partners making decisions or taking action against individuals in ways that can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private?
- Will the project require you to contact individuals in ways that they may find intrusive?
- References: UK's Information Commissioner's Office, International Association of Privacy Professionals (IAPP)

Conclusions

- Data protection and privacy are complex issues.
- There is no one-size-fits-all approach that can be applied to these areas.

Thank you!