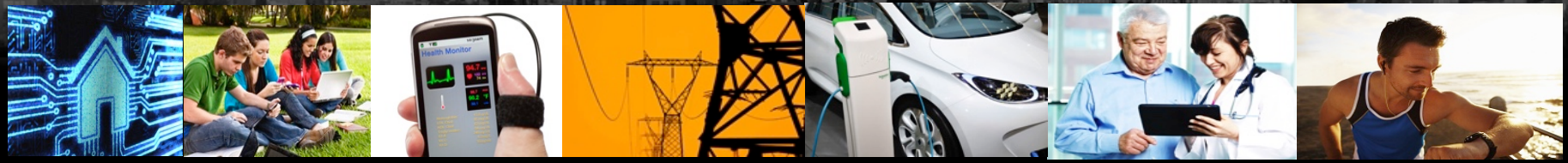
Connected Living

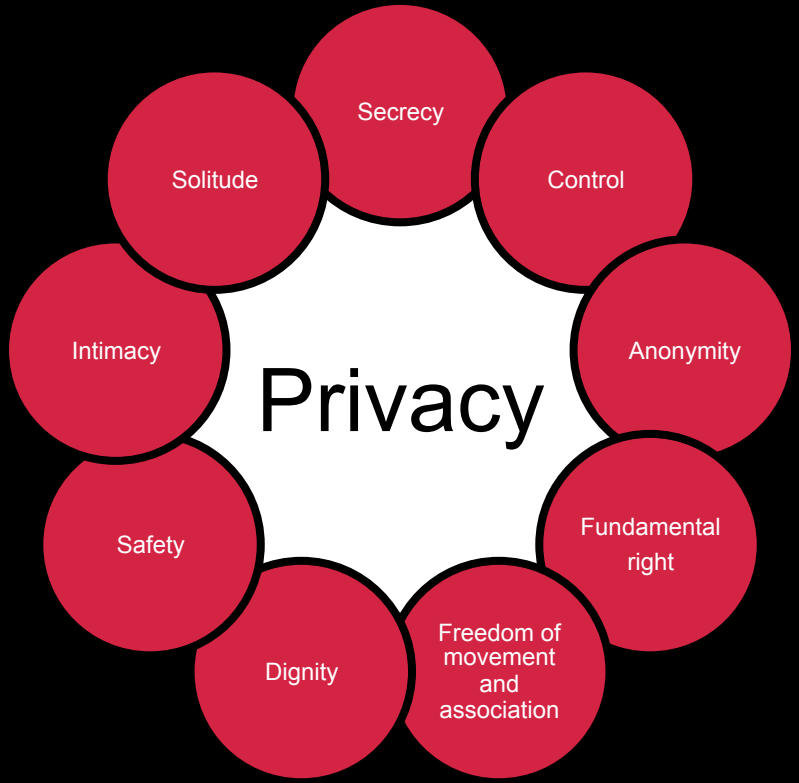


Building trust and respecting privacy in the 'Internet of Things' – An introduction

Yiannis Theodorou – Senior Manager, Regulatory & Public Policy, GSMA

- Mobile and IoT Privacy: Key considerations
- Key privacy challenges in consumer IoT space
- Conclusions and recommendations

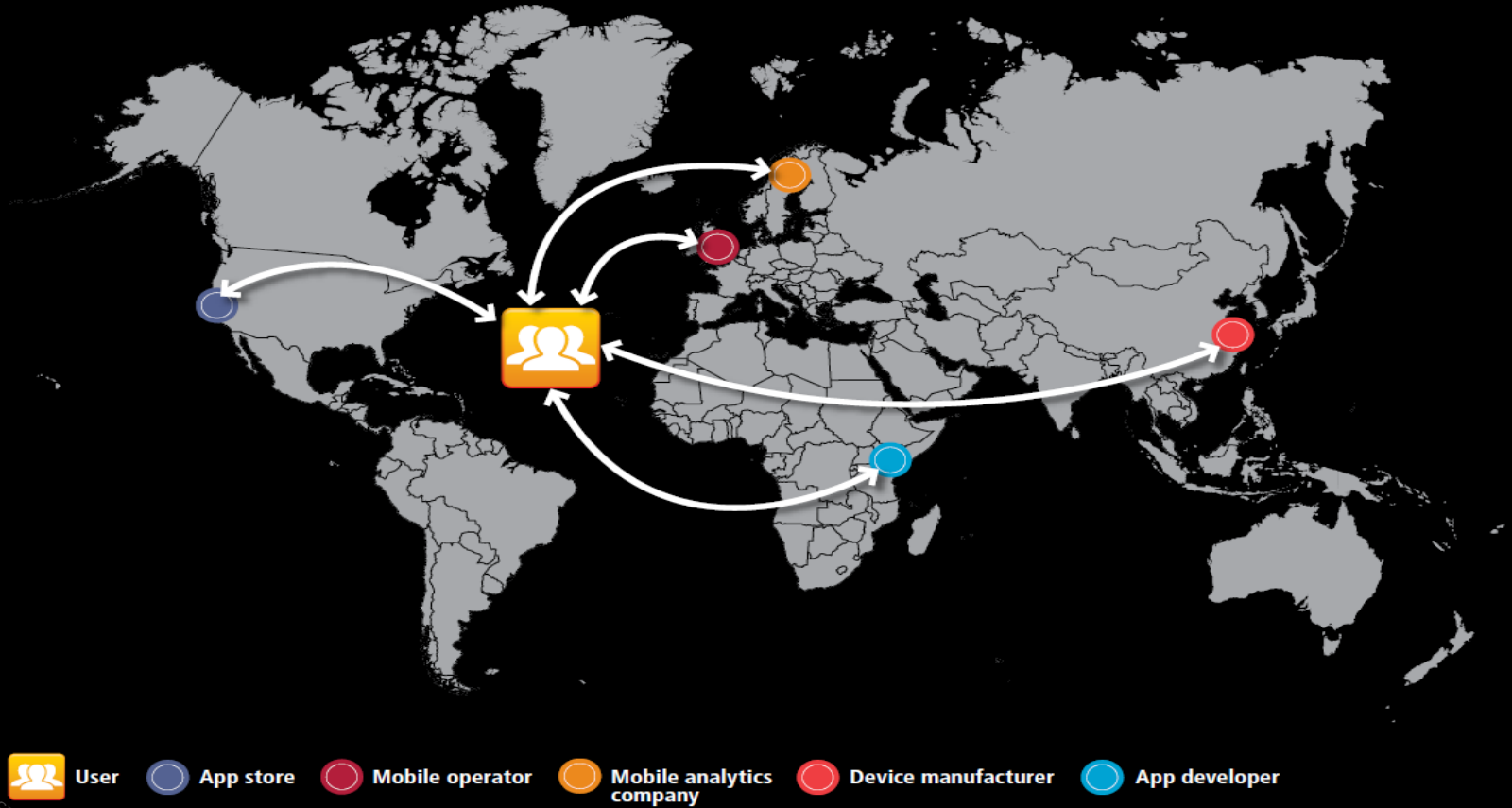
Privacy – What does it mean?



Mobile privacy on an internet – enabled device

- Broadcasting data by default
- Real time data collection / sharing
- Always on

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



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

The IoT will involve more connected sensors and devices which means:

- More data created and collected in real time, often without user awareness
- Accessed or shared by a potentially unlimited number of companies
- Better data analytics = **more insights**

'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 gathers data about water temperature and correlates this with fish stock
- A cash-only vending machine that sends stock and machine-status info only

Mobile privacy on an internet – enabled device

Many IoT services can directly improve people's lives…

… But can also lead to negative consequences...

- Possible financial impact on consumer including price discrimination
- Impact on freedom of expression, movement and association
- Privacy concerns may drive people away from the benefits IoT technologies can offer

Security is NOT the same as privacy

- Good Security =
  - Ensuring data is secure both in transit and at rest (when stored)
  - Ensuring the confidentiality, integrity and availability of data
- Good Privacy =
  - Appropriate collection & use of information
  - Being transparent with individuals
  - Respecting rights & choices of individuals
  - … and always depends on context

- Mobile and IoT Privacy: Key considerations
- Key privacy challenges in consumer IoT space
- Conclusions and recommendations

Challenge 1: Data protection laws apply to ‘personal data’…but non-personal data can *also* impact privacy

Data protection laws set out **rules** that seek to protect privacy by:

- Placing obligations and restrictions on the collection and use of 12‘**personal data**’
- Requiring consumer consent to process some categories of personal data e.g. health information
- **Changing definitions of ‘personal’ data**
  - ‘Personal data’ is any info relating to an *identified* or *identifiable* living, natural person

BUT!

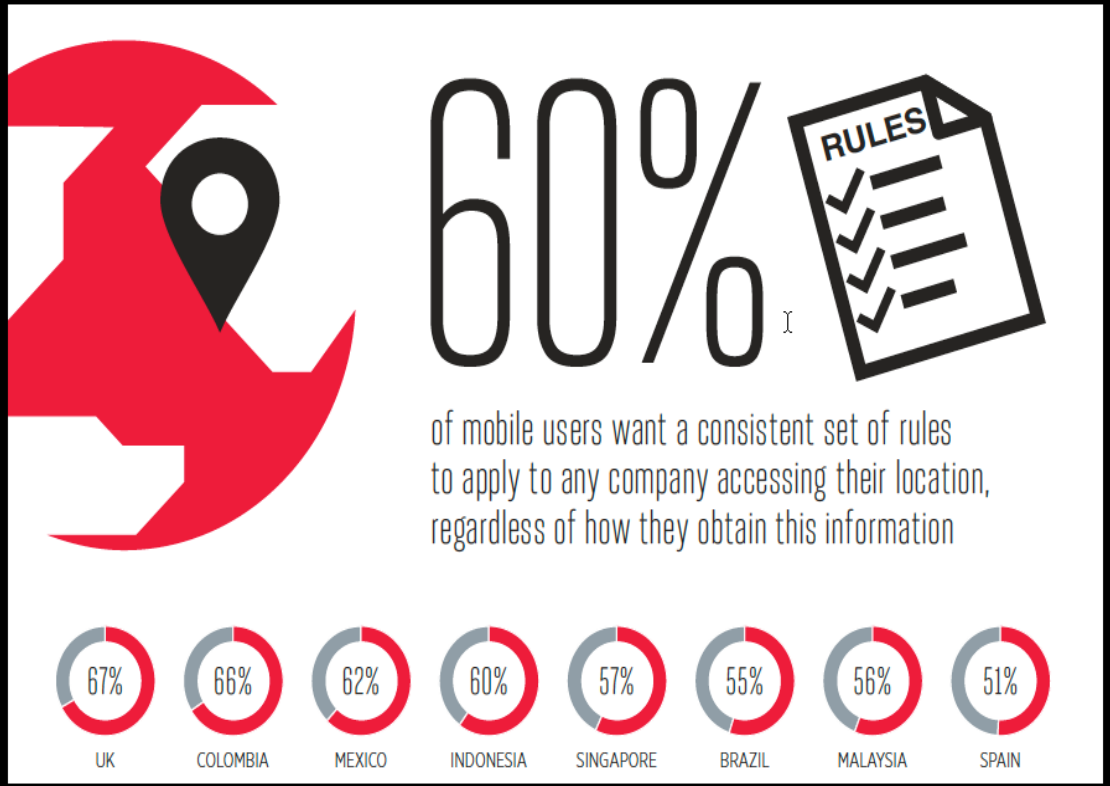
- The analysis of data obtained from consumers’ connected devices may have real privacy and other implications on their lives, even if not considered ‘personal’ in law

Challenge 2: Multiple and often inconsistent privacy regulations, or none at all !

Challenge 2 (cont'd): Focus on location data

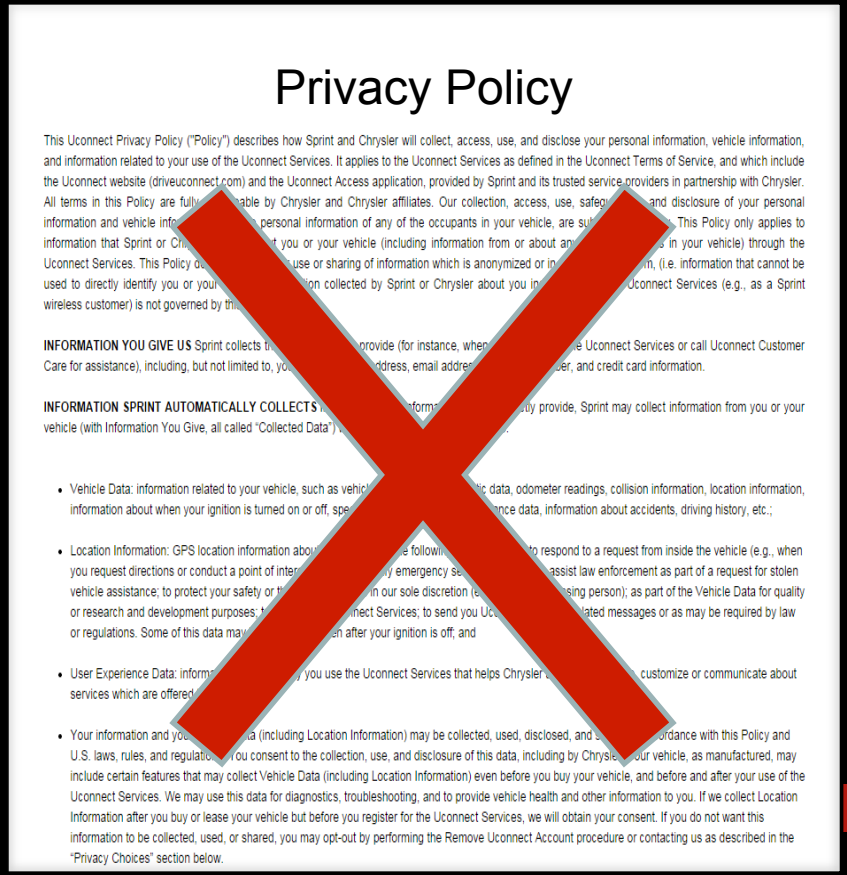
- What is location?
  - Where I am now + activity/context?
  - Where I am not (normally)?
  - Where I am heading?
  - Where I have been?
  - Which route have I travelled?
  - Which way I am facing / what is my elevation?
  - What people and things I am connected to?

Challenge 2 (cont'd): inconsistencies in regulating location data is affecting consumers and businesses



- Cellular location and traffic data are often regulated and their use restricted
- The equivalent traffic processed by Internet companies — W-Fi and GPS location data — is not regulated or restricted
- This has implications for:
  - Users
  - Businesses
  - Big Data
  - Governments

Challenge 3: ‘Buried’ Ts&Cs no longer meet consumers’ or policymakers’ expectations



Privacy Policy

This Uconnect Privacy Policy ("Policy") describes how Sprint and Chrysler will collect, access, use, and disclose your personal information, vehicle information, and information related to your use of the Uconnect Services. It applies to the Uconnect Services as defined in the Uconnect Terms of Service, and which include the Uconnect website (driveuconnect.com) and the Uconnect Access application, provided by Sprint and its trusted service providers in partnership with Chrysler. All terms in this Policy are fully [illegible] able by Chrysler and Chrysler affiliates. Our collection, access, use, safeg[illegible] and disclosure of your personal information and vehicle info[illegible] personal information of any of the occupants in your vehicle, are su[illegible]. This Policy only applies to information that Sprint or Chr[illegible]t you or your vehicle (including information from or about an[illegible]s in your vehicle) through the Uconnect Services. This Policy d[illegible] use or sharing of information which is anonymized or in[illegible]n, (i.e. information that cannot be used to directly identify you or your[illegible]on collected by Sprint or Chrysler about you in[illegible] Uconnect Services (e.g., as a Sprint wireless customer) is not governed by thi[illegible]

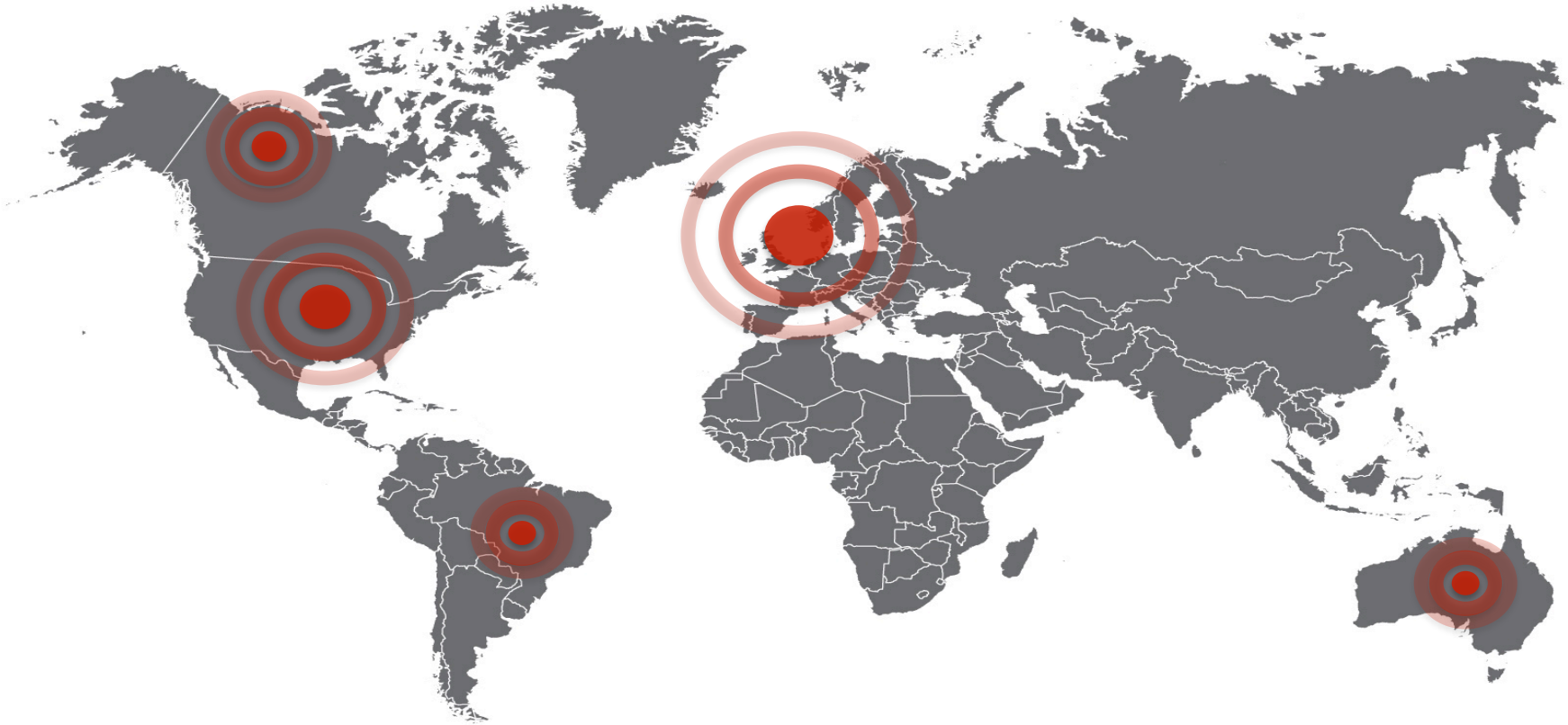
INFORMATION YOU GIVE US Sprint collects t[illegible] provide (for instance, when[illegible]e Uconnect Services or call Uconnect Customer Care for assistance), including, but not limited to, yo[illegible]ddress, email addre[illegible]er, and credit card information.

INFORMATION SPRINT AUTOMATICALLY COLLECTS [illegible]nform[illegible]ly provide, Sprint may collect information from you or your vehicle (with Information You Give, all called "Collected Data") [illegible]

- Vehicle Data: information related to your vehicle, such as vehic[illegible]ic data, odometer readings, collision information, location information, information about when your ignition is turned on or off, spe[illegible]nce data, information about accidents, driving history, etc.;
- Location Information: GPS location information abou[illegible]e followi[illegible] to respond to a request from inside the vehicle (e.g., when you request directions or conduct a point of inter[illegible]y emergency se[illegible]assist law enforcement as part of a request for stolen vehicle assistance; to protect your safety or t[illegible]in our sole discretion (e[illegible]sing person); as part of the Vehicle Data for quality or research and development purposes; t[illegible]nect Services; to send you Uc[illegible]lated messages or as may be required by law or regulations. Some of this data may[illegible]n after your ignition is off; and
- User Experience Data: inform[illegible]y you use the Uconnect Services that helps Chrysler [illegible], customize or communicate about services which are offered[illegible]
- Your information and yo[illegible]a (including Location Information) may be collected, used, disclosed, and s[illegible]ordance with this Policy and U.S. laws, rules, and regulatio[illegible]you consent to the collection, use, and disclosure of this data, including by Chrysle[illegible]our vehicle, as manufactured, may include certain features that may collect Vehicle Data (including Location Information) even before you buy your vehicle, and before and after your use of the Uconnect Services. We may use this data for diagnostics, troubleshooting, and to provide vehicle health and other information to you. If we collect Location Information after you buy or lease your vehicle but before you register for the Uconnect Services, we will obtain your consent. If you do not want this information to be collected, used, or shared, you may opt-out by performing the Remove Uconnect Account procedure or contacting us as described in the "Privacy Choices" section below.

Many ‘IoT’ / connected devices lack a User Interface (Screen) – no privacy policy / settings?

IoT Privacy has captured the attention of policymakers across the world



Areas of particular interest to policymakers

- User awareness and control
- Understanding and addressing privacy risks in specific contexts
- Companies' **compliance and accountability** in relation to data protection and privacy
- **'Anonymisation' of** data, where appropriate?
- How to balance **encryption**, users' privacy & lawful government access to information?
- Setting appropriate **sanctions**

European policymakers are leading the way towards strengthening data protection rules – others following?

The new 'GDPR' is intended to apply to any company targeting European citizens

- Creates a set of **harmonised rules** across all EU member states
- Introduces **fines** of up to 5% of company's annual global turnover
- Strengthens obligations to provide **information and choice** for consumers
- **Stricter requirements on consent: must be explicit, prior and informed**
- **Requires Data Protection 'by Design' and 'by Default'**
- **Requires impact assessments**
- Encourages support for **privacy certifications**/seals/'icons'
- Extends the definition of personal data (to include **location data**, device identifiers)
- Gives individuals the **right to data portability**
- Extends **data breach notification** to all sectors (not just telcos)

How can companies maintain consumers' privacy in a connected world?

- The GSMA developed a few core privacy principles that all companies dealing with consumers' data should consider ***before*** launching a service or product

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

- The GSMA has also developed an 'IoT Privacy Design Decision Tree' to illustrate the key privacy considerations for providers of a new IoT service (see separate attachment)

- Mobile and IoT Privacy: Key considerations
- Key privacy challenges in consumer IoT space
- Conclusions and recommendations

Conclusion: Why privacy?

WHAT IS IT REALLY ABOUT?

It's about strengthening consumers' **TRUST** in a service or brand name

It's about **RESPECTING LAWS & CONSUMERS' RIGHTS** and expectations

It's about industry **SELF-REGULATION** and mitigating unwarranted and restrictive laws

WHAT DOES IT MEAN FOR IOT SERVICE PROVIDERS?

- Higher uptake of service / less churn
- Better reputation for service provider
- Higher brand loyalty

- Respecting consumers' rights/expectations
- Committing to / implementing best practices
- Non-compliance with privacy & data protection laws can lead to fines, sanctions, and reputational damage

- Proactive and effective industry-led measures are necessary to minimise the need for formal regulation which may impact innovation and revenues
- Allows flexibility to respond to new threats

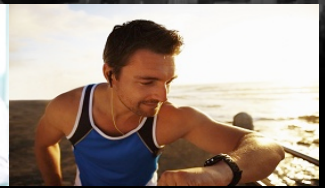
Conclusion: Recommendations

- IoT Service Providers
  - → Consider consumers' privacy when initially designing a service/product
  - → Collaborate with partners to ensure end-to-end privacy
- Software developers and UX/UI designers
  - → Offer tools that enable the consumers to control their privacy settings
- Policymakers
  - → Adopt a risk based approach and incentivise industry self-regulation
- Data Protection Authorities
  - → Provide independent guidance and promote global best practices

Connected Living





Yiannis Theodorou
Senior Manager, Regulatory & Public Policy, GSMA

YTheodorou@gsma.com, @yiathe