



Connected
Living



Building trust and respecting privacy in the 'Internet of Things'

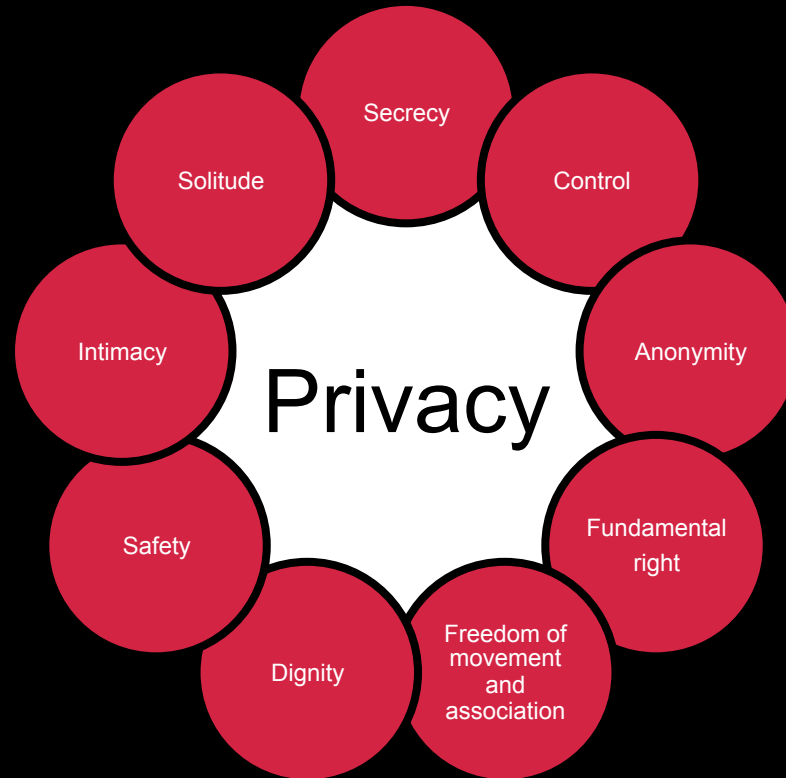
Yiannis Theodorou – Senior Manager, Regulatory & Public Policy, GSMA

Objectives of today's seminar

- To outline:
 - Mobile and IoT Privacy: Key considerations
 - Key privacy challenges in consumer IoT space
 - The GSMA's IoT Privacy by Design Decision Tree
 - Conclusions and recommendations
- Q&A
- ... NOT a 'legal & compliance' webinar...

- Mobile and IoT Privacy: Key considerations
 - Key privacy challenges in consumer IoT space
 - The GSMA's IoT Privacy by Design Decision Tree
 - Conclusions and recommendations

Privacy – What does it mean?





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



User



App store



Mobile operator



Mobile analytics company



Device manufacturer



App developer

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

Connected Living – Mobilising the Internet of Things

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
- The GSMA's IoT Privacy by Design Decision Tree
- Conclusions and recommendations

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



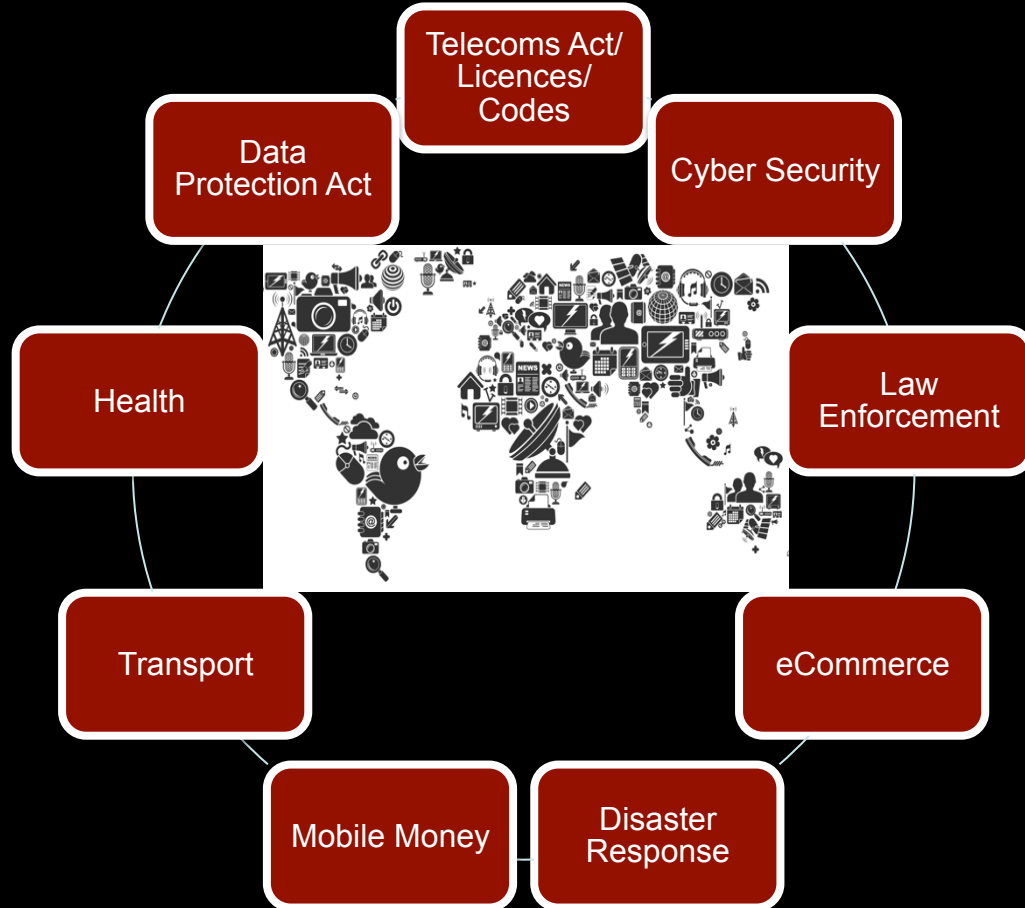
Data protection laws set out **rules** that seek to protect privacy by:

- Placing obligations and restrictions on the collection and use of **‘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?

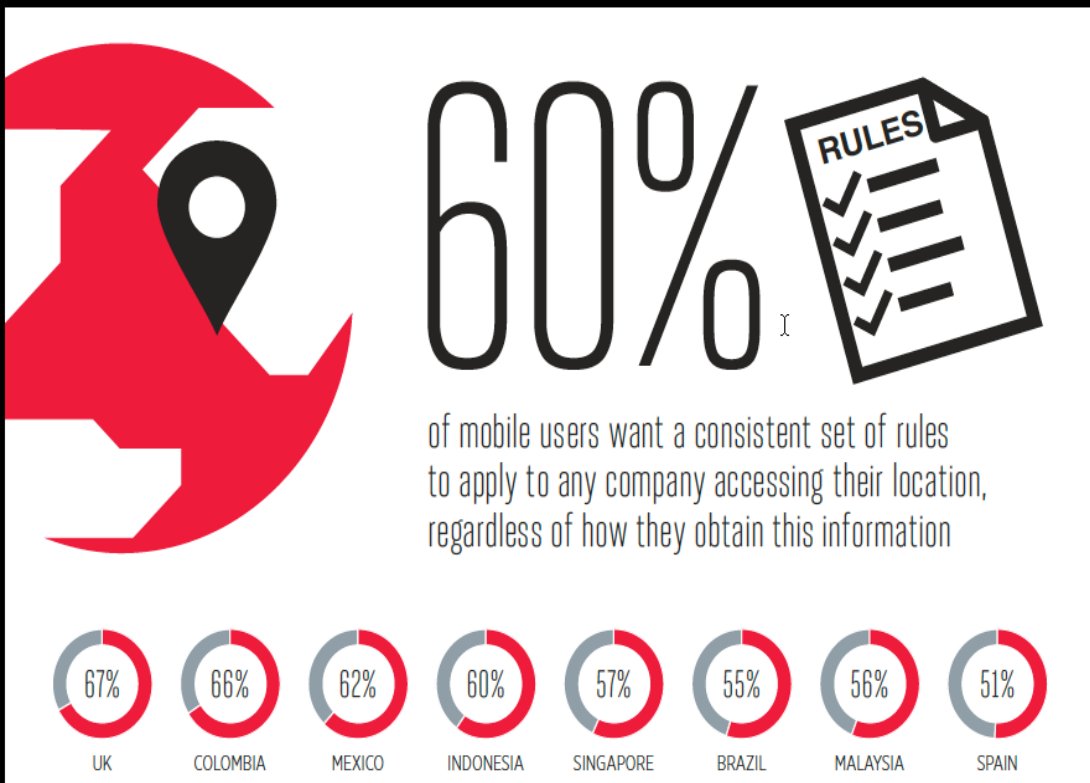
Where I have been?

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

Connected Living – Mobilising the Internet of Things

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 enforceable by Chrysler and Chrysler affiliates. Our collection, access, use, safety, and disclosure of your personal information and vehicle information, including personal information of any of the occupants in your vehicle, are subject to this Policy. This Policy only applies to information that Sprint or Chrysler collect from you or your vehicle (including information from or about any person or persons in your vehicle) through the Uconnect Services. This Policy does not cover the collection, access, use, or sharing of information which is anonymized or aggregated information, (i.e. information that cannot be used to directly identify you or your vehicle) or information collected by Sprint or Chrysler about you in connection with Uconnect Services (e.g., as a Sprint wireless customer) is not governed by this Policy.

INFORMATION YOU GIVE US Sprint collects the information you provide (for instance, when you use Uconnect Services or call Uconnect Customer Care for assistance), including, but not limited to, your name, address, email address, phone number, and credit card information.

INFORMATION SPRINT AUTOMATICALLY COLLECTS When you use Uconnect Services, information you automatically provide, Sprint may collect information from you or your vehicle (with Information You Give, all called "Collected Data")

- **Vehicle Data:** Information related to your vehicle, such as vehicle identification number, vehicle data, odometer readings, collision information, location information, information about when your ignition is turned on or off, speed, engine data, information about accidents, driving history, etc.;
- **Location Information:** GPS location information about your vehicle. We may use the following information to respond to a request from inside the vehicle (e.g., when you request directions or conduct a point of interest search), to provide emergency services, to assist law enforcement as part of a request for stolen vehicle assistance; to protect your safety or the safety of others; in our sole discretion (e.g., to assist a law enforcement officer in identifying a person); as part of the Vehicle Data for quality or research and development purposes; to send you Uconnect Services; to send you Uconnect Services; to send you Uconnect Services; to send you Uconnect Services; or as may be required by law or regulations. Some of this data may be collected even after your ignition is off; and
- **User Experience Data:** Information about how you use the Uconnect Services that helps Chrysler and its service providers to customize or communicate about services which are offered to you.
- **Your information and your vehicle data** (including Location Information) may be collected, used, disclosed, and otherwise processed in accordance with this Policy and U.S. laws, rules, and regulations. You consent to the collection, use, and disclosure of this data, including by Chrysler and its service providers, your 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?

Connected Living – Mobilising the Internet of Things

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)

Connected Living – Mobilising the Internet of Things

- Mobile and IoT Privacy: Key considerations
- Key privacy challenges in consumer IoT space
- The GSMA's IoT Privacy by Design Decision Tree
- Conclusions and recommendations

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



GSMA's IoT Privacy by Design Decision Tree



Initial interaction / activation
of service/product

1 What data is
needed/collected?

2 Is Data “personal”
& regulated in law?

YES

“Black or white” –
Straightforward compliance

NO

6 Could the use of
data impact an
individual’s privacy?

YES

NO

*E.g. will it be shared with 3rd parties or used for
purposes non-obvious to the user?*

3 How will data be
used & what for?

4 Conduct Privacy
Impact Assessment
(PIA)

5 Design User
Interface: Transparency
Choice & Control

4 Conduct Privacy
Impact Assessment
(PIA)

**CONSUMER TRUST
IN THE IOT SERVICE
IF IT MEETS:**

**(I) PRIVACY & DATA
PROTECTION
OBLIGATIONS**

**(II) CONSUMER
PRIVACY RIGHTS**

**(III) CONSUMER
PRIVACY
EXPECTATIONS**

Decision Tree: 1. What data do you need & how will you collect it?



Service/product activation

1 What data is needed/collected?

- What data do you need to collect from/about the consumer so that your IoT service or product can function properly?
 - 'static' Vs 'dynamic' data
- Will data be collected automatically or through consumer's manual sign-up?
- How will you obtain the consumer's consent/permissions in relation to using such data e.g. through:
 - The registration form? Online webpage? Smartphone app?
 - Other media interface?
 - What if your device only has sensors but no screen? (see also step 5)

See Steps 2-6 →

Have you considered the consumer-journey when designing the activation process? Do consumers understand how their data will be used across the value chain & the impact, if any, to their privacy?

Decision Tree: 2. Is Data “personal” & regulated in law? (compliance and due diligence)



2 Is Data “personal” & regulated in law?

- What is the definition of “personal” data in each of the markets you operate in?
- Is the data collected “personal” & regulated in law? If so, have you identified the legal basis that allows you to process such data?
- Are you subject to any privacy-related licence conditions (e.g. telco)
- Are there any federal, state, local or sector-specific laws that apply in addition to general data protection laws? e.g.:
 - Financial / payment services, healthcare regulations
 - Potential restrictions on cross-border data transfers

Decision Tree: 3. How will data be used & what for? (compliance and due diligence)



3 How will data be used & what for?

- Is data kept secure both when stored and transmitted?
- Clearly set out the data flow: Identify how the data will be used and shared across the value chain and for what purposes
- Justify why the data is needed in specific context
- Define/agree privacy responsibilities with your partners from the outset (and ensure the product design reflects these)
 - Contractual agreements (e.g. limiting the use of data by Analytics providers for their own commercial purposes)
 - Consider Principles / Codes of Conduct / Guidelines

Decision Tree: 4. Conduct a Privacy Impact Assessment (Assessing and mitigating risk)



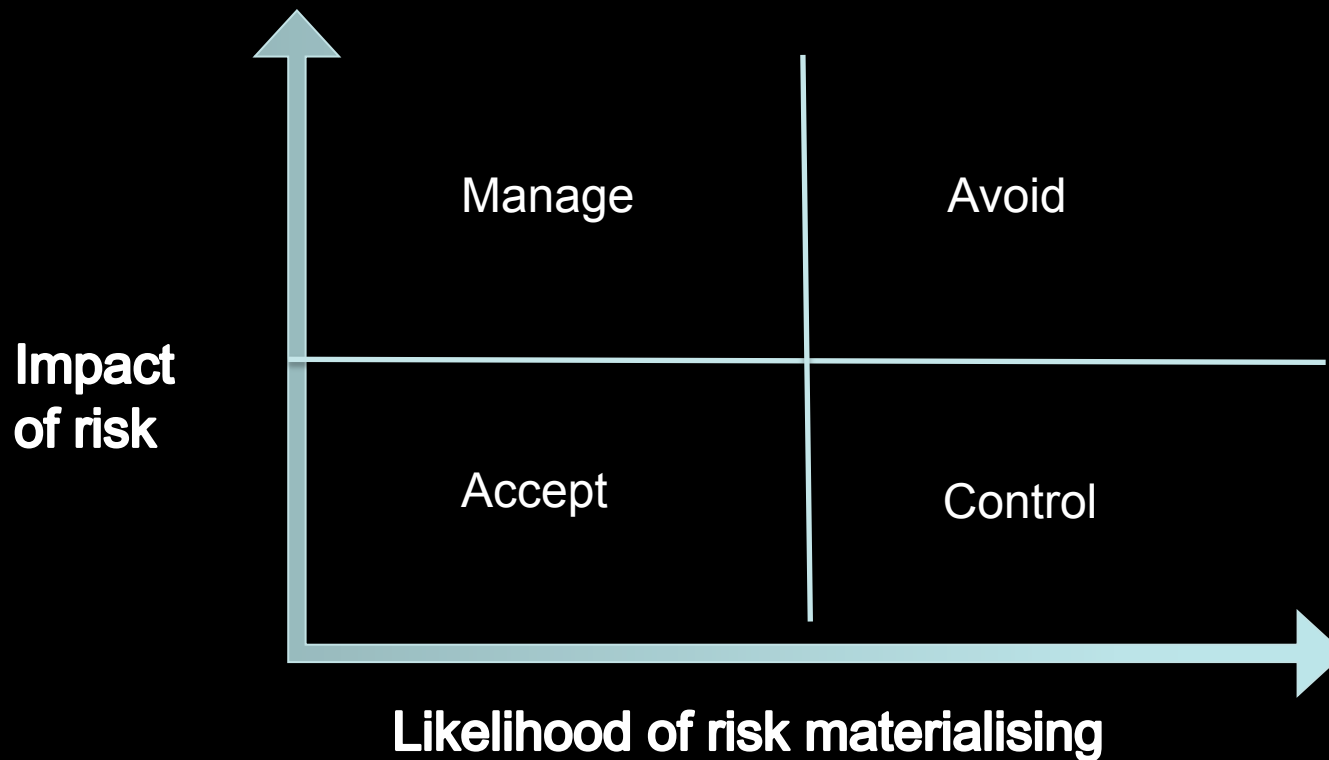
4 Conduct Privacy Impact Assessment (PIA)

- 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 \(IAPP\)](#)



Decision Tree: 4. Conduct a Privacy Impact Assessment – cont'd (Assessing and mitigating risk)



Decision Tree: 5. Design User Interface (Transparency, Choice & Control)



5 Design User Interface: Transparency Choice & Control

Have you met your obligations and consumers' rights in law... but also their expectations? e.g.:

- Is the consumer aware?
- Can they make informed choices?
- Have you obtained their consent? (where legally required)
 - Key elements of consent include: disclosure, comprehension, voluntariness, competence, agreement)
- Is data secure in transit and at rest?
- Is there a set period for which consumer data will be kept?

Does the consumer journey help gain their trust?

- Can consumers express their privacy preferences in simple steps e.g. via
 - web 'permissions dashboard', 'just-in-time' prompts, a call centre, a mobile app, a voice activated command etc.

Decision Tree: 6. Could the use of data impact an individual's privacy?



6

Could the use of data impact an individual's privacy?

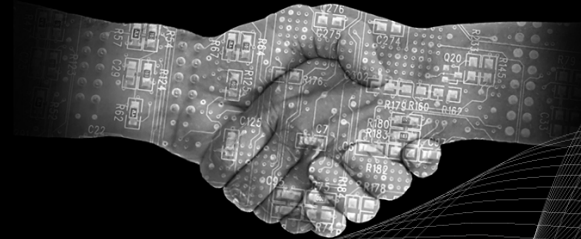
Even if the data is not defined as 'personal'...

- Could the data be used to impact an individual's privacy? For example:
 - Could (non-personal) data from your service/product be combined with other data from different sources to draw inferences about a consumer's lifestyle and impact on his/her ability to get health insurance...Or price discriminate against the consumer?
- **What happens if your service changes in the future?** For example:
 - Functionality of device or service changes (e.g. starts to collect consumers' location data)
 - Data or customer profiles shared/sold to 3rd parties (e.g. advertisers) who start using consumer data for different purposes than those originally obtained for
- **If any such changes occur you should:**
 - Check possible impact on your business if new laws are invoked as a result of change
 - Establish processes to inform the consumers and obtain their consent where necessary
 - Provide the means for consumers to change their privacy preferences

Decision Tree: 6. Could the use of data impact an individual's privacy? (cont'd)



- Have you considered the roles/responsibilities of all your IoT partners For example:
 - partner mobile operator(s)
 - device manufacturer(s)
 - SIM vendor(s)
 - Service delivery platform owner(s)
 - Other 3rd party in the value chain ?
- Who does the customer expect to be responsible for their personal data and who would they turn to if things go wrong?
 - Have you an agreement in place with your partners on how privacy complaints or concerns should be handled?



- Mobile and IoT Privacy: Key considerations
- Key privacy challenges in consumer IoT space
- The GSMA's IoT Privacy by Design Decision Tree
- 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

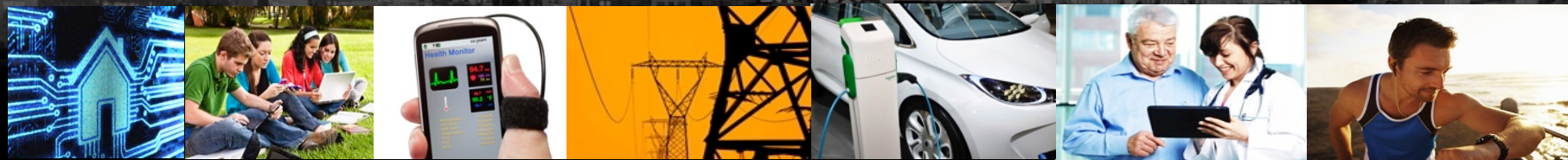
Conclusion: Recommendations

- 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

Questions?



Thank you
Yiannis Theodorou
Senior Manager, Regulatory & Public Policy, GSMA

YTheodorou@gsma.com, @yiathe