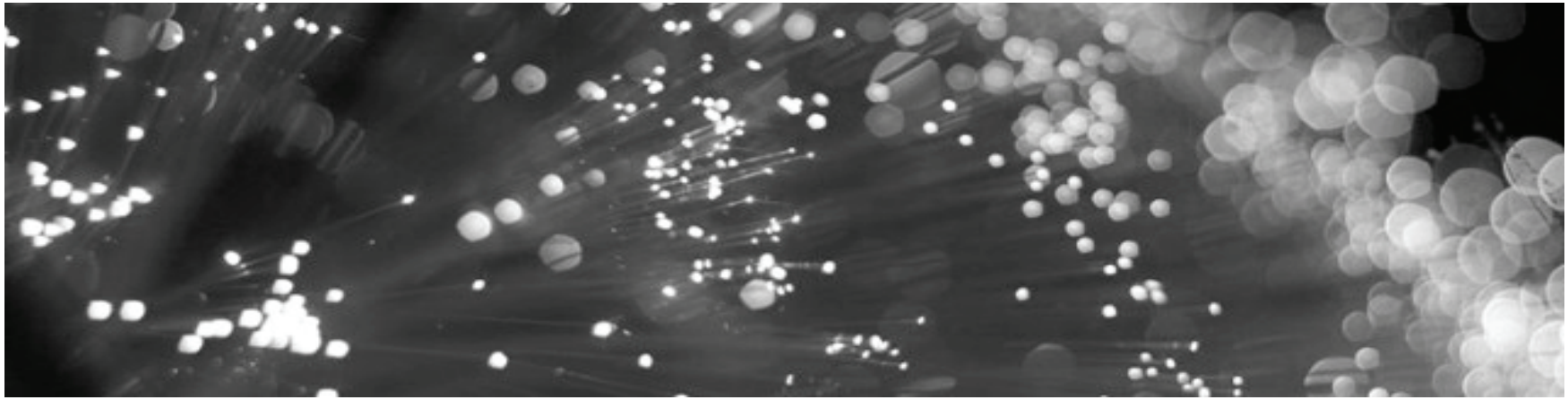
NORTON ROSE

FINANCIAL INSTITUTIONS
ENERGY
INFRASTRUCTURE, MINING AND COMMODITIES
TRANSPORT
TECHNOLOGY AND INNOVATION
PHARMACEUTICALS AND LIFE SCIENCES

Machine-to-Machine Communications

Opportunities and Risks

Nick Abrahams
Partner and Asia-Pacific Technology Leader
Norton Rose Australia
October 2011



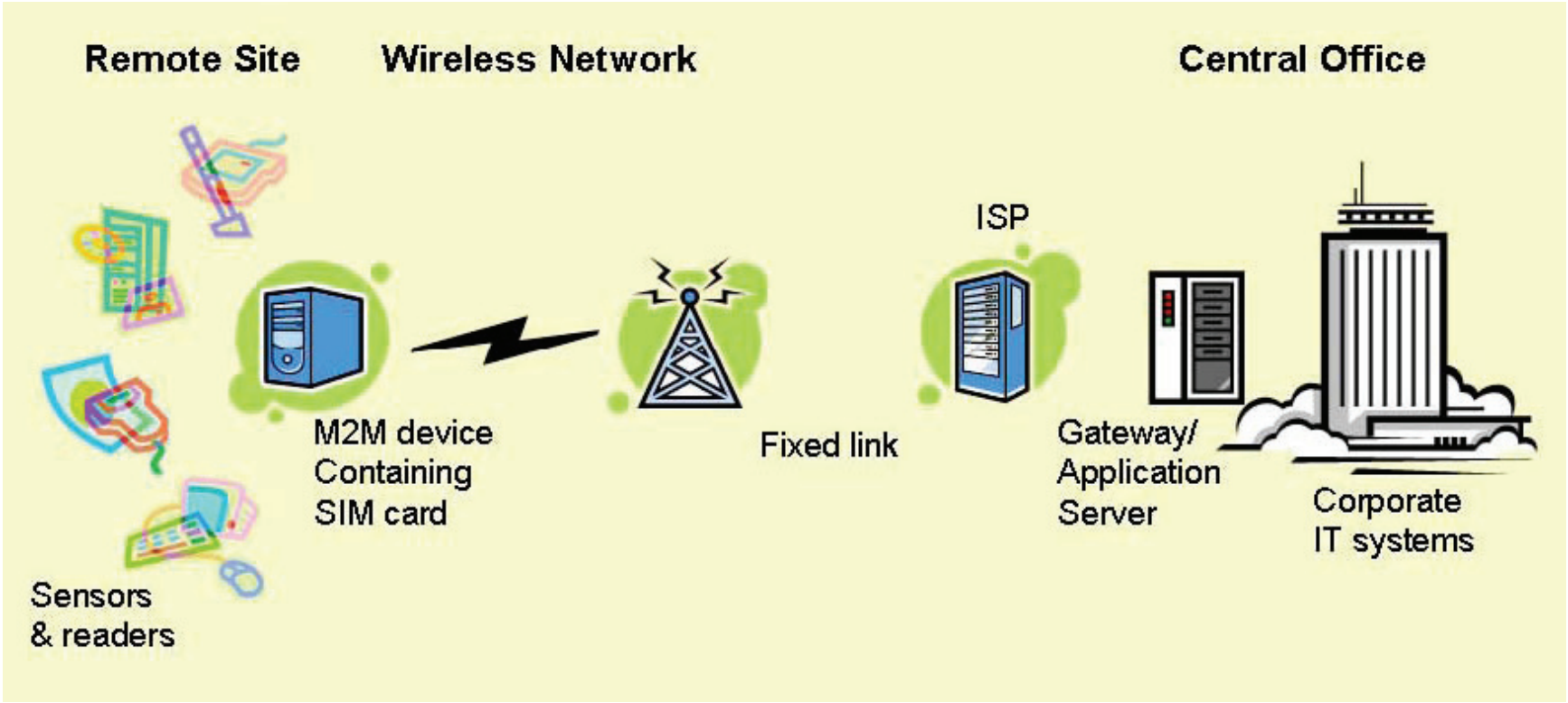
Today

- What are the opportunities for M2M?
- What are the commercial risks?
- What are the legal risks?

What is M2M - Definition

- M2M uses a *device* (such as a sensor or meter) to capture an *event* (such as temperature or inventory level) which is relayed through a *network* (wireless, wired or hybrid) to an *application* (software program), that translates the captured event into *meaningful information* (such as which items need to be restocked)
- “Embedded devices” or “Embedded connectivity”
- Low data usage (but over many years) so 2G is okay. 1 smart phone = 10,000 embedded devices
- Move from ARPU to Margin per Machine
- Allows for remote upgrading of software

Components of a Wireless M2M System



NORTON ROSE

Examples of M2M

- Automatic meter reading (from wirelessly-enabling electricity, water or gas meters to car parking)
- Geo-fencing / fleet management – monitoring devices to verify location of heavy equipment (eg. mine trucks)
- Inventory control – from refilling vending machines to maintaining optimal inventory vs cost status
- Healthcare monitoring
  - home-based wellness monitoring – informational and critical care
  - pace maker reports on heart conditions
- Remote security management – video needs high bandwidth
- Track compliance with legislation
  - Heavy goods vehicle compliance in EU
  - Remote highway toll collection (Germany)
  - EU eCALL INITIATIVE – all cars have GSM/GPS to enable auto-emergency calls (↑ in stolen vehicle tracking services)

NORTON ROSE

Examples of M2M

- Product transportation tracking
- Automotive – breakdown call, emergency call, pay as you drive insurance, stolen vehicle tracking, speed monitoring between fixed points
- Parking sensors to aid the driver and vehicle to vehicle communication to prevent accidents or avoid traffic jams
- Machine preventative maintenance
- Livestock health monitoring, soil conditioning, pollution monitoring and prevention

NORTON ROSE

What is M2M - Usage and Growth

- Consulting firm Analysys Mason forecasts that the number of M2M device connections will grow from **62 million** in 2010 to **2.1 billion** devices in 2020 (36% year-over-year growth rate)

- Juniper Research forecasts that M2M will support industry revenues of over **$35 billion** in 2016

- Major offering by all major telcos globally

M2M risks

- Lack of M2M device control once deployed. South African traffic light SIMs
- M2M devices not necessarily valued by consumers in the same way they own and look after their mobile phones
- Ability to modify M2M device will enable fraud (SIM cloning)
- The situation where M2M usage is not controlled or monitored until something actually goes wrong Impact of millions of unsecure devices attached to the network (eg. washing machines)?

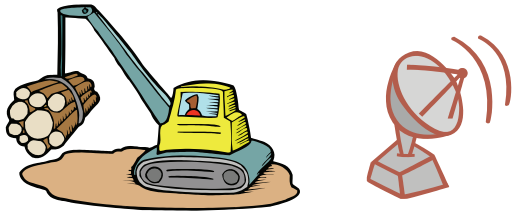
NORTON ROSE

Legal risks

- Spectrum use – whether M2M applications require dedicated spectrum
- Fraud and security – digital and physical protection
  - Malware, devices unattended
- Privacy – personal and commercial information
  - Vehicle tracking data or medical records accessed by insurance investigators
- Lack of human monitoring – spread spectrum alarm monitoring issue
- Performance – Telcos used to “best efforts” and now business / life critical
- Multiple SIMS – Customer gets 4 embedded devices = 4 SIMS = 4 Accounts? Or on one plan with one collective data cap?
  - Purchase connectivity with device (eg. Kindle or GPS sat nav)
- How to churn the CSP? Also multiple SIMS = multiple accounts
- Value chain – Who brings the value – CSP, managed service provider, device owner
  - More strategic partnerships and reliance on third parties
- CSPs supply data to law enforcement and provide lawful intercept

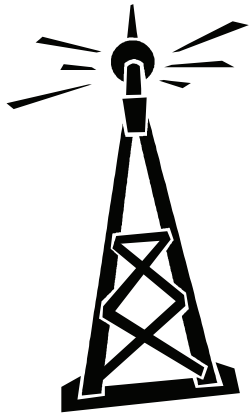
M2M legal issues – Case Study 1 – Geo-fencing

Example



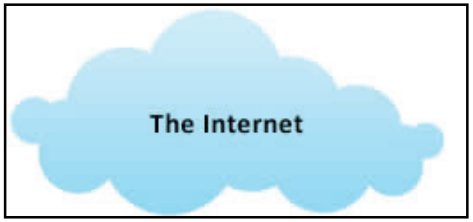
Equipment monitored by Device

Device sends information to Mobile Base Station over wireless network



Mobile Base Station

Mobile Base Station sends information through the Internet



User accesses information via website to monitor equipment remotely

User

NORTON ROSE

Geo-fencing case study

Radiocommunications licences

- Vehicle manufacturer gets into new business of providing geo-fencing
- Transmitter device – class licence restrictions
- Importers and manufacturers of M2M device need to comply with both the Radiocommunications and Telecommunications Acts:
- Ensure compliance with each applicable Australian Standard at the required compliance level
- Make and hold a Declaration of Conformity
- Prepare and maintain compliance records eg test reports, drawings and circuit diagrams etc
- Label the device as required:
  - obtain a supplier code number from the ACMA
  - C-Tick label
  - A-Tick label

Case study 2 – Surveillance tracking

Surveillance legislation

- Model legislation prepared in 2005
- Intended that all States and Territories would enact model legislation to ensure uniform approach to surveillance across Australia
- Not all States and Territories have enacted legislation based on model legislation
- In NSW, NT, VIC and WA - similar legislation relating to the use of surveillance devices applies across these jurisdictions
  - Prohibition on use of “tracking devices” without consent. Consent can be express or implied
- In SA, TAS, ACT and Qld - legislation based on model legislation has not been enacted, or has only been partially adopted, in these jurisdictions
  - No separate offence in relation to the use of tracking devices
  - Arguably consent not required to passive location services in these states
- Odd result

Case study 3 – Smart meters

- Privacy is key as are concerns about which parts of the chain (or competitors) should get access to data
- Australia required specific legislation to allow network operators the right to install the meters (retailers generally do don't)
- What type of technology can keep these devices connected for 20 to 30 years?
- California new privacy legislation for consumer's energy use data:
  - Disclosure - utilities cannot share customer's energy use data without consent
  - Data security / protection – utilities must protect data for access and the Act prohibits "the use of data for a secondary commercial purpose"
  - Continued use – utilities are granted permission to continue using customer data for analysis, reporting and program management
  - Liability – utilities that release data to a third party with consent are not liable for the misuse of the data

Case study 3 – Smart meters (cont)

German energy industry law - smart metering

Amendment to German energy industry law came into force on 4 August 2011

- comprehensive implementation of smart metering is one of the main objectives (Sect. 21c EnWG)
- contains a complex set of rules regarding privacy and data protection aspects
- these include rules on technical and organisational measures that have to be taken
- Particular requirements for technical systems shall be defined (privacy by design)
- Specific provisions for data processors (eg M2M solution providers)

Case study 3 – Smart meters (cont)

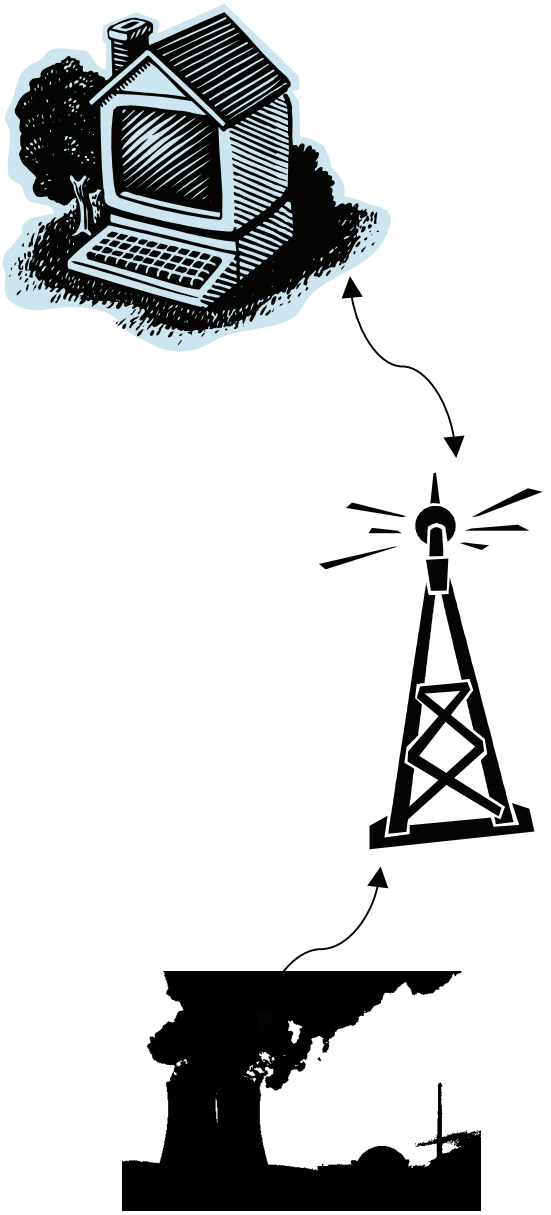
UK Smart Metering - Background

- Roll out of UK Smart Metering Programme to be completed by 2019
- More than 50 million electricity and gas meters
- £11 Billion investment
- Central programme managed by Dept of Energy and Climate Change
- Government currently undertaking Foundation Stage
  - Metering technical specification will be finalised
  - Suppliers will procure test and roll out meters
  - Establishment of the Data Communications Company
- Mass Roll out commences in 2014

Case study 3 – Smart meters (cont)

Role of the Data Communications Company

- A new licensed entity responsible for procurement and contract management of data and communications services
- UK Government will run a competitive process for the DCC licence
- Role
  - Initially those activities which are “essential for the effective transfer of smart metering data”
    - Secure communications
    - Access control
    - Scheduled data retrieval
    - Translation services
  - Procuring necessary equipment and services to provide WAN Communications including WAN Module
  - Subsequent role of meter point/supplier service registration
  - DCC will facilitate access to smart meters by network operators



NORTON ROSE

Conclusions

- M2M is here and growing
- Risks are manageable
- Legal risks will be challenging
- Regulatory considerations
  - Use to enforce law (eg. travel time, etc.)
  - Privacy
  - CSP churn
  - Law enforcement obligations
- Non-telcos affected