Internet of Things, Big Data, Cloud:

Take Security and Privacy seriously to stay in the game

Coupled with social media and mobility, three lines of enabling technologies are converging

■ Internet of Things (IoT)

- IoT devices are being integrated into a wider and wider variety of products
- Huge amounts of data are being generated by those devices
- Vast numbers of use cases cover all industries sectors and aspects of our lifestyle from retail to healthcare, transportation to entertainment.

■ Big Data

- Datasets can now be processed that have different complex structures
- Technology is capable of correlating efficiently huge amounts of complex data from diverse datasets to produce meaningful information in a timely manner

■ Cloud Computing

- Commoditised computing resources provide flexibility, scalability and cost-efficiency around processing power, memory, persistent storage and networking
- Massive data processing is available at very low cost to anyone connected to the Internet

Convergence of IoT, Big Data and Cloud Computing is opening up a very large number of possibilities in terms of digital products and services

Those will impact every aspect of our lives and – over time – change society

It is not just hype : This type of technology convergence has a profound transformational potential

- **Technology convergence is creating a true paradigm shift**
  - – The number of use cases is HUGE
  - – This is not about ‘techie’ gadgets and “funny” apps anymore but devices, concepts and services which have the potential to provide real benefits and value to large populations of consumers
  - – It is impacting all industries and reaches deep into our lifestyle
  - – It could affect everything we do in ways comparable to the deployment of electricity grids 100 years ago

McKinsey – The Internet of Things: Mapping the Value Beyond the Hype

The economic value created by IoT (alone) is predicted to be $3.9 - $11.1 trillion per year in 2025

- **However …**
  - – At the intersection of technologies and in the midst of the proliferation of use cases, privacy has become vulnerable
  - – And fundamental cybersecurity principles – if ignored – will lead to breaches and data losses that may damage consumer confidence

The topic has been gaining widespread media recognition

- **Three examples taken from the UK mainstream press that illustrate privacy and security challenges**

RETAIL: How tracking customers in-store will soon be the norm

“At the Fairson's department store, managers can measure the number of people who walk past the store, the number who come through the front door – and this information includes whether or not they went in immediately or were convinced by the shopfront.

Once shoppers are inside the store, managers can find out how many of them walked up to the second floor and compare with the number of people who took the journey to the second floor last week.

If more people have gone up this week, they'll probably conclude that the marketing banners that they put up towards the beginning of the week are working.”

“What about consumer’s privacy ?”

Source: The Guardian 10/1/2014

http://www.theguardian.com/technology/datablog/2014/jan/10/how-tracking-customers-in-store-will-soon-be-the-norm

CONSUMER ELECTRONICS: Home, Hacked Home

“One night in April a couple in Ohio was woken by the sound of a man shouting, “Wake up, baby!” When the husband went to investigate, he found the noise was coming from a web-connected camera they had set up to monitor their young daughter while she slept. As he entered her bedroom, the camera rotated to face him and a string of obscenities poured forth.”

“There are just super simple flaws in some medical devices,” says Billy Rios of Qualys, a cyber-security firm. Last year he and a colleague found “back doors” into various bits of medical equipment. These are passwords used by technicians from firms that sell the devices to update the software that runs them. A hacker with a back door could use it to, say, adjust an X-ray machine so that it administers a far higher dosage than its display shows. Mr Rios took his findings to regulators and worked with them and with the companies involved to fix the flaws.”

“In January Proofpoint, a security firm, claimed it had found evidence that a group of compromised devices, including home routers, televisions and a refrigerator, had been commandeered by hackers and were being used to pump out spam.”

Source: The Economist – 12/7/2014

http://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home

AUTOMOTIVE: Connected car – what can it actually do?

“The EU has ruled that from October 2015 all new cars and vans in member countries must be fitted with a telematics system called eCall. Designed to transmit the vehicle’s location to emergency services in the event of a crash, the system comes with a built-in M2M SIM and an SOS button near the dashboard so drivers can call 999 quickly. If airbags are deployed eCall automatically sends a text message to emergency services with the car’s location and its unique vehicle ID number.”

“Many cars are already starting to incorporate “intelligent” technology for everything from remote diagnostics to internet access for online entertainment and dedicated apps for controlling the vehicle remotely. For example, Volvo’s On Call not only provides roadside assistance inside the car if it breaks down, but also features an Apple/Android app which enables you to control the car both from outside as well as inside. For example, with the app you can check your car’s fuel level, battery level, maintenance warnings and more. Doors can be locked and unlocked, the car can be started remotely and its heating set to the required temperature.”

Source: The Telegraph – 25/11/2014

http://www.telegraph.co.uk/sponsored/technology/4g-mobile/machine-to-machine/11252473/connected-car-what-does-it-do.html

IoT – It is not about “things” : It’s a really about People

- **Most valuable use cases revolve around devices used by people**
  - IoT devices and concepts are being embedded into more and more products used by people; on that basis, a large variety of additional services can be created and offered to consumers based on their usage, behaviour, location etc…
  - Adoption of products with embedded IoT devices – or services built on such data – will depend on the value that the consumer perceives in relation to those services
  - Consumers are used (willingly or not) to trading personal data in exchange of Internet services perceived as free

Personal Data has been the real currency of the “free” Internet for years

- **At the same time, people have expectations of security and rights of privacy**
  - At least in most of the developed world, but with very significant sociological and legal variations
  - IoT devices can be hacked but simple cybersecurity measures (e.g. complex default passwords, shutting down unused ports) will go a long way to protect
  - Embedding “secure by design” principles as early as possible in the development of IoT products and services, and proper thorough testing prior to release are essential

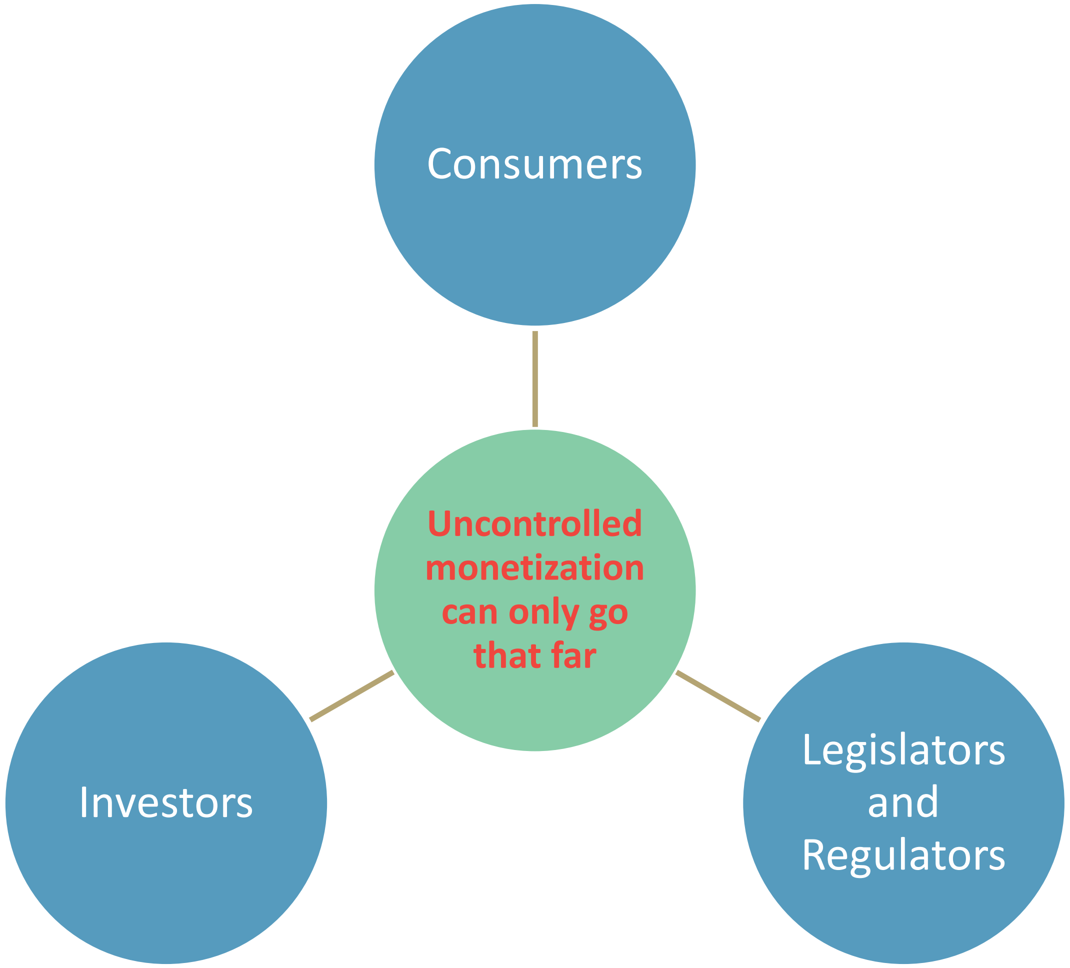
Big Data – Data is the new Oil

- **Data is a raw commodity, from which many Information products can be derived**
  - Data alone is relatively value-less but Big Data technology enables its efficient processing
  - Processing complex data (like refining crude oil) transforms it into a large number of valuable information-based sub-products
  - The correlation of different datasets – with different formats, structures, schemas – allows more sophisticated and useful information-based products to be created, which in turn can be traded and processed (e.g. into reports, dashboards etc…)
- **At every step in the data transformation chain, there can be value creation**
  - Data may be used or sold for additional purposes that were not envisaged when it was collected
  - The sale of IoT data may become a business line in itself for some organizations but sensitive personal data must be identified and protected
- **This is a fundamental new phase in the Information Age**
  - IoT devices have exponentially increased the volume and types of data that are available
  - The number of combinations and use cases is enormous if you can obtain the necessary data

But the ruthless monetization of Personal Data can lead to consumer rejection and – over time – destroy value

Several strong forces will act over time to control the extent of monetization

Consumers will react negatively to blatant abuse like they have done in the past (e.g. against the abuse of SMS text messaging) and social media give them greater power than ever to act against abusive patterns


Consumers
Uncontrolled monetization can only go that far
Investors
Legislators and Regulators

Investors will continue to demand coherence in business models

Legislators are likely to step in where the privacy of citizens is threatened and will develop regulations further if/when they do

Failure to find a self-regulatory balance will lead to value destruction

The mechanics of value destruction

- **Consumers have greater-than-ever powers to act directly against companies not taking security or their privacy into account**
  - They may stop buying products or services, if they think their personal data is being or might be misused; they may hide behind proxies
  - Social media give individuals a powerful platform to develop global campaigns against large corporations
  - Privacy-related themes have been gaining wider and wider media interest over the past years – at least in the developed world
  - The reputational and economic impact of a media campaign gaining traction can be significant
- **The challenge is global for large corporates**
  - Consumers have different expectations based on their nationality, culture, age, education, etc… and the legal and regulatory context also varies from country to country
  - Issues in one geography can impact operations in another
  - Cross-border legal cases may be complex and precedents may drive abrupt changes in legal frameworks, as highlighted by the CJEU rulings around the “Safe Harbour” principle in October 2015
- **Governments may feel obliged to intervene**
  - Unhappy citizens may demand action
  - Politicians may have to legislate to control an undesirable situation and increase regulation further

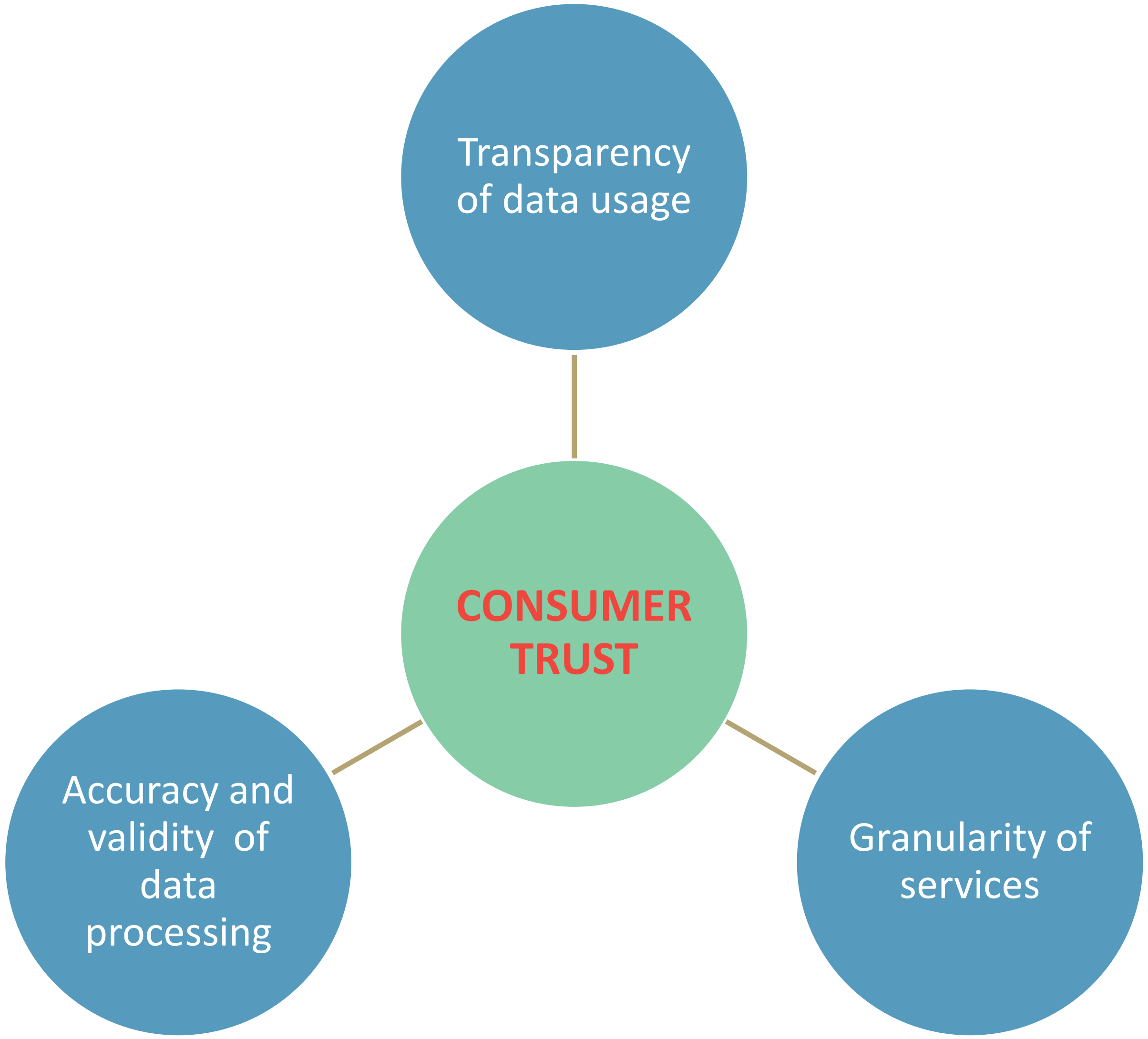
Looking ahead

- **Over the long term: By the 2030s, the digital transformation of society should have happened**
  - There is simply too much value being created and too many use cases
  - Security and privacy concerns will destroy some economic value over time but this will not be sufficient to de-rail the paradigm shift because of its fundamental underlying transformational potential
- **In the short term: Up to 2020, security and privacy failures will create significant disruption and unpredictable tensions**
  - Until a self-regulatory balance is found
  - In the meantime, good security and privacy practices are likely develop into a key competitive advantage
- **The key message to Executive Management:**

Take security and privacy seriously NOW and embed good practices into your products and services to avoid being an early casualty and remain competitive over the long term

Building Trust

- **Long-term acceptance of the digital products and services emerging from the technological convergence will rely on building trust and credibility with the consumers**


Transparency of data usage
CONSUMER TRUST
Accuracy and validity of data processing
Granularity of services

Transparency of the data usage

- **What data is being collected and how it will be used and protected must be clear**
  - It must be communicated to the consumers in a way and in a language they will understand i.e. in the context of their own expectations in terms of security and privacy
  - This is a complex problem as consumers may have different expectations based on their nationality, culture, age, education etc…
- **Legal agreements must be clear**
  - Current “click-through” agreements are too long and too complex; virtually no one reads them in their current form; who retains ownership of the data is not clear
  - As a result, their enforceability may be dubious in many cases and is likely to challenged at some stage

Providing short plain language summaries of legal and data usage agreements should develop into a fundamental good practice for all service providers

Granularity of the services

- **Consumers must be given some choice based on their privacy expectations**
  - Today, most services are provided in a binary manner: Either you agree to a user agreement you don't understand and over which you have no influence, or you cannot access the service
  - Some organisations are trying to provide more choices but these have not really provided meaningful options yet
  - Again, this is a complex problem for global organisations as consumers may have different expectations based on their nationality, culture, age, education etc…

- **Providing tiered services based on privacy expectations will increase acceptance**
  - But it has to be meaningful and embedded in the way the service is conceived and delivered
  - A repeat of the implementation of the EU "Cookie Laws" must be avoided as it has turned into a meaningless "tick-box" exercise for consumers

Taking consumers privacy expectations seriously and not just as a mere compliance exercise is essential to long-term acceptance

Accuracy and validity of the data processing

- **Identifying individuals accurately is key to many use cases**
  - For many use cases, it is key to ensure that multiple identities for a single individual are only linked together if it is certain that it is the same physical person
  - But, not all data generated by IoT devices or collected from other sources will be attributable to an specific individual
  - What to do if & when there is any doubt ?
- **Failure to maintain data integrity could destroy value**
  - It is key to understand whether the available data is the raw data from the original sources or not, as data can be manipulated through the various transformations it has to undergo
  - If identity becomes confused and data from multiple individuals are presented as belonging to a single individual, then any results will be meaningless
  - In the event of the data be transformed and some aspect being changed, the conclusions reached from using that data may be flawed
- **Statistical, sociological and scientific theory must remain paramount**
  - Data availability and processing capabilities allow the delivery of countless use cases but results have to be valid in their specific context
  - It should be the role of the Chief Data Officer and of Data Scientists to ensure the true accuracy and validity of processing, but for that, they have to be and remain “scientists” with a problem to solve; not marketing people looking for data soundbites to maximise sales
  - Manipulating data to reach a pre-established outcome will damage credibility

The absence of underlying processing integrity will only destroy trust

Key lines of actions for Executive Management to stay in this game over the long term

- **Embed Security good practices and “secure by design” principles at the start of the product design cycle**
  - Do it NOW to gain competitive advantage
- **Respect consumers expectations of privacy to build trust**
  - Offer consumers fair and plain terms in a language they can understand
  - Be open about how their data will be used and protected, and make sure the measures you commit to are put in place
  - Offer meaningful services granularity aligned with privacy expectations of various groups of consumers
  - Respect geographical, sociological & generational differences
- **Respect the integrity of data and the integrity of use cases to build credibility**
  - Appoint a Chief Data Officer and Data Scientists with the right background, to ensure that the underlying processing model is sound, technically and scientifically

Contact

For further information please contact:

Jean-Christophe Gaillard
Managing Director
+44 (0)7733 001 530
jcgaillard@corixpartners.com

Neil Cordell
Director
+44 (0)7701 015 275
neilcordell@corixpartners.com

www.corixpartners.com

Many thanks to our focus group members, contributors & reviewers

Focus Group

- **Rupert Brown**, CTO Financial Services at MarkLogic
- **Paul Ferron**, Digital Identity Strategist EMEA at CA Technologies
- **Frederic Halley**, Europe Operating Partner at Next World Capital
- **Jean-Marie Lapeyre**, EMEA CISO at General Motors
- **Matt Saxon**, Enterprise Architect at Worldpay
- **Alastair Upton**, Chief Technology Officer at ATG Media

Other contributors and reviewers

- **Francois Gratiolet**
- **John Leach**
- **Blandine Marcelin**