Role of Data Privacy on International Business: Innovating for Consistency Within Regions & Beyond

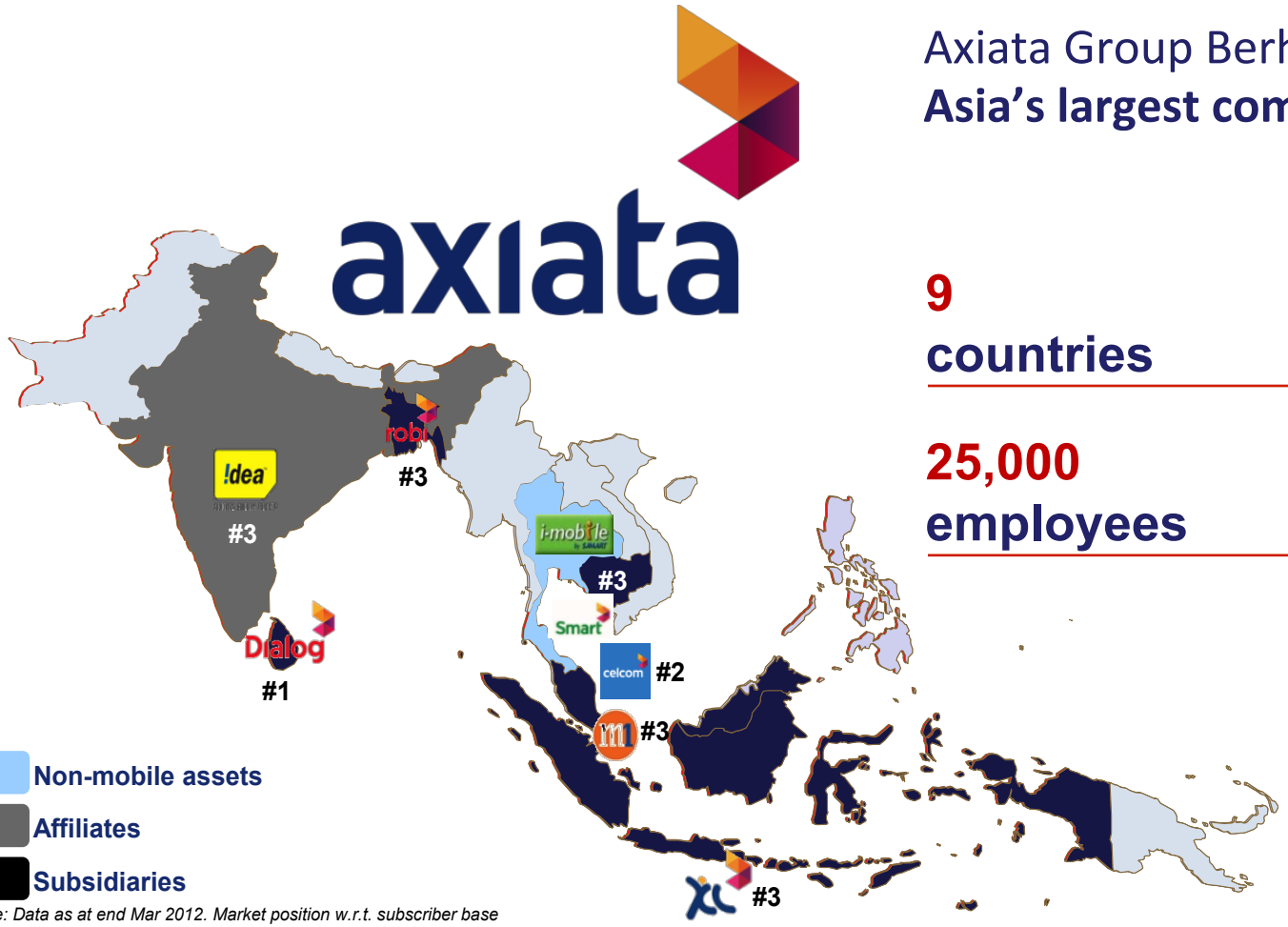
GSMA Data Protection and Privacy Conference

Kuala Lumpur

August 2013

Rob Borthwick
Axiata Group Berhad

About Axiata



Note: Data as at end Mar 2012. Market position w.r.t. subscriber base

Axiata Group Berhad (Axiata) is one of **Asia's largest communications companies**.

9 countries	**215 million customers**
25,000 employees	**USD 5.7 billion revenue in cash (2012)**

Axiata aspires to be an Asian **regional champion by 2015: *Advancing Asia.***

Consumers have concerns about Data Privacy

GSMA Consumer Research

- Carried out in three Asia-Pacific markets including Singapore, Indonesia and Malaysia
- And internationally in Europe and South America
- Suggesting broadly similar consumer concerns regarding the treatment of customer data by commercial concerns

"Mobile internet users have privacy concerns and want to know their personal information is safe:

- ***80%+*** *have concerns about sharing personal information when accessing the internet of apps from a mobile; but*
- ***60%+*** *would continue to use apps regardless; and the*
- ***30%+*** *with concerns would use these services more if they felt their information was safeguarded better."*

Typical customer personal information concerns:

- Credit card / financial service details
- Personal information from social networking profiles
- Mobile location / mobile number

But sharing of personal data by consumers is increasing dramatically:

- Because technology is changing and spreading
- Because of the value of the on-line service experience to consumers
- Because other people – friends, family and celebrities - are doing this.

Service Terms and Conditions / Privacy Policies are used to inform consumers:

- But lengthy Terms and Conditions don't grab customers' attention
- Relationship between customers and immediate providers may be clear [or may not]
- Less customer clarity where there are 3rd parties and where data is held internationally.

Policy makers are responding: we see proliferation of national Data Protection Laws and Regulation in Asia Pacific

Some jurisdictions in Asia Pacific have enacted comprehensive data protection laws

New Zealand; Hong Kong; Taiwan; Australia; South Korea; Japan; Macau; Philippines; Singapore

Other countries have developed their own legislation or draft legislation or have started consultation processes

India; Malaysia; China; Vietnam; Indonesia; Thailand;

Some countries are revisiting / revising / strengthening current laws

South Korea; Taiwan; New Zealand; Australia; Hong Kong; Macau

Still no laws in certain countries but expect this to change in the future

Brunei; Cambodia; Laos; Sri Lanka; Bangladesh

Source: Asia Pacific Data Privacy – 2011 Year of Revolution, Updated by Axiata

And there is a long history of development of personal data protection responses internationally

OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data – 1980

- Eight principles of data privacy and security: collection limitation, data quality, purpose specification, use limitation, security, openness, individual participation, accountability.
- Non-binding among members, resulted in unequal implementation.

Council of Europe Convention for the Protection of Individuals - 1981

- Principles that personal data should be obtained fairly and lawfully, stored for specified and legitimate purposes, adequate, relevant, not excessive, accurate and stored only as long as necessary.
- Provisions for sensitive data (religion, political beliefs, genetic or medical information).

European Data Protection Directive – 1995

- Introduced to reconcile the right to privacy with the right to information and to ensure similar protection across EU
- Revisions now being discussed include developments in the technological and globalised world, setting up a general EU framework for data protection, and a Directive to protect personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

APEC Privacy Framework – 2004

- Nine principles of data privacy and security: preventing harm, notice, collection limitation, use limitation, choice, integrity, security, access and correction, accountability.
- Guidance on domestic as well as international implementation between member economies.

Madrid Resolution – 2009

- Developed to encourage internationally uniform protection of personal data and facilitate international flows of personal data in a globalizing world by integrating legislation from all five continents. Follows 6 principles (lawfulness and fairness, purpose, proportionality, data quality, openness, accountability).

However, increasing innovation is dramatically changing forms of supply and enabling new consumer services

- The mobile *"app"* economy is dramatically changing the way that consumers are using services and are expanding the range of services being consumed - innovation

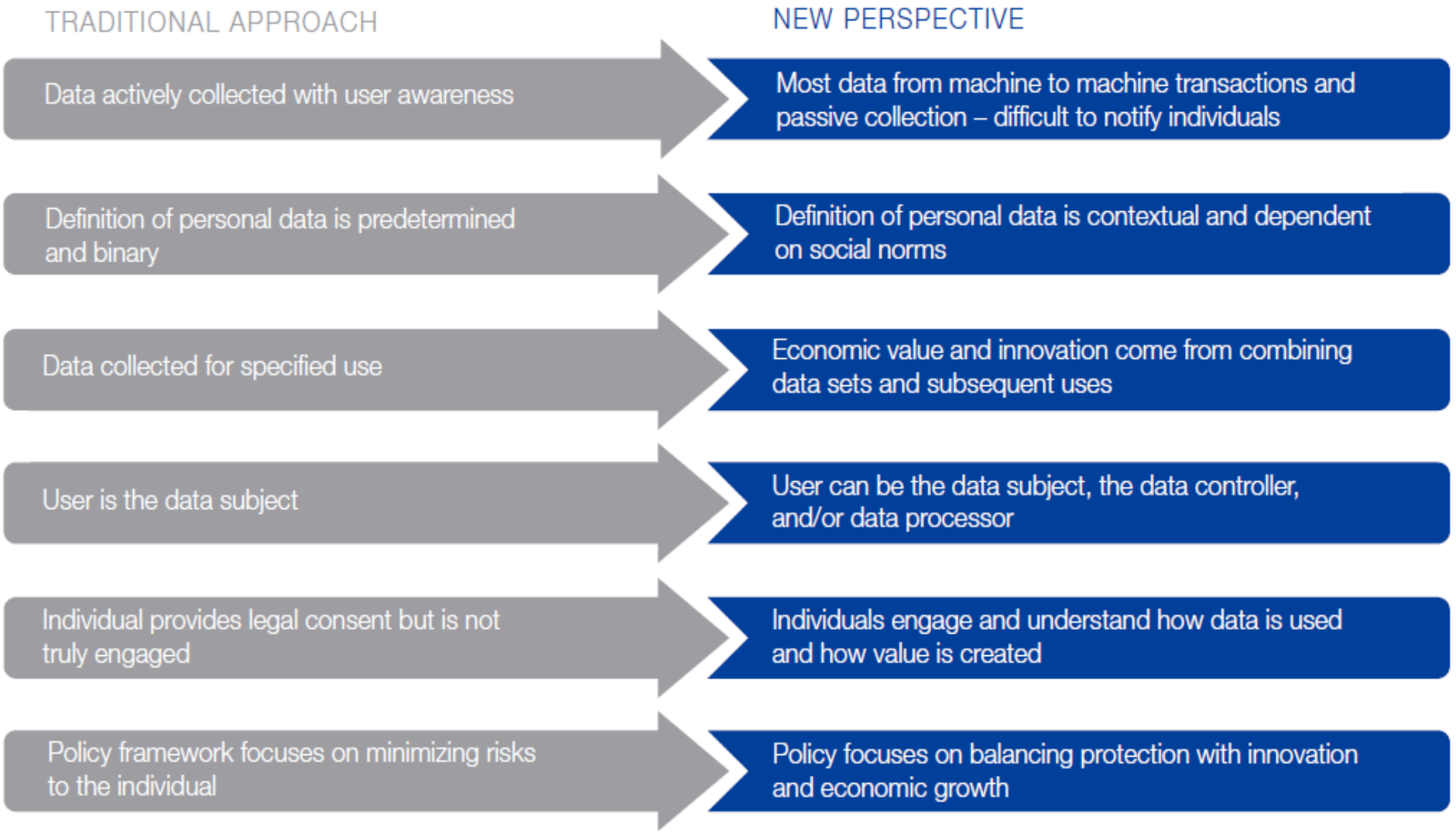
- Suppliers see that the full potential of current and future services cannot be realised without consumer trust and confidence. This includes the security of on-line transactions and information networks and the privacy of customer information.

- While service models differ, new services will not be produced by nationally-focussed producers – to a traditional *"telco"* model. Instead, as previously with manufacturing, we are seeing a transition to international production and multi-national consumption.

- In this context data protection frameworks which are consistent and interoperable internationally support international distribution and low unit costs – which translate into low prices.

- Inconsistency of national privacy regulation applies asymmetrically – affecting different industries and types of providers in different ways. Some of this difference is proportionate to concerns and risks. Some, however, looks back to legacy regulatory frameworks, rather than forward to a globally connected World.

And we should anticipate further acceleration of new uses (and approaches to the use) of personal data



Source: World Economic Forum, Boston Consulting Group, 2013

Internationally consistent data privacy supports innovation and consumer benefit

- Personal data can be used for social and commercial opportunities by a large number of innovators, and the rate of new service offerings and novel social and business models is high.
- A consistent international framework will address divergent regulatory developments in multiple jurisdictions where legislation varies by country and by type of supplier.
- Effective regional (and ideally global) frameworks will guide efforts to produce proportionate commercial data privacy while not stifling innovation or down-playing the potential value of socially and commercially appropriate data-sharing.
- The global dimension of commercial data privacy policy requires close attention, not only to enable the flow of commerce, but also to prevent conflicting policy regimes acting as trade barriers.
- APEC and other international bodies provide the forum for agreeing on data privacy policy principles which – though trade commitments – can steer the world toward global privacy protection interoperability through mutual recognition of each others' commercial data privacy systems and cross-border regulatory cooperation.
- National legislative and regulatory responses to data privacy should be pragmatic and reflecting common data privacy principles (and consumer concerns). With national market responses developed through co-regulatory mechanisms – such as sectorial codes of practice.

To support new approaches, solutions must be both practical and effective

Communications permission	Spectrum permission	VAS provider code *[for example]*
• Single set of rules for commercial operation of communications networks and services Without service or technology distinctions • Communications determine the boundary of their operations on a commercial basis. • Industry co-regulation customizes horizontal concerns for the sector.	• Simple description of spectrum which is being made available to a provider or which is unlicensed • With terms which deal ***only*** with spectrum-related issues, e.g. period of allocation, payment terms, management of interference. • Again without service or technology distinctions	• A code which is managed by the NRA / Value Added Services-(VAS) regulator • With terms which deal ***only*** with VAS pricing, transparency, etc. • VAS providers register and must be in good standing to offer services and to contract with communications licensees • Industry co-regulation

National legislation consistently dealing with horizontal concerns including data privacy – with proportionate co-regulation by sector

Internationally consistent data privacy principles