Data Privacy and Data Security : What is Most Likely to Bring a Company's Business to a Halt

Sylvia Fang
Vice President and General Counsel
TSMC Ltd.

June 15, 2015

Agenda

- Overview of Issues
- Privacy and Compliance
- Data Breach: A Clear and Present Danger

Overview of Issues

- **With cyber-intrusions and attacks increasing in both prevalence and sophistication, data (including personal data) security is a pressing concern for all businesses.**
- **67% of 5,000 corporate executives believed that their GC/legal department could most benefit from additional expertise in the area of cybersecurity** *(Survey — GCs: Adding Value to the C-Suite, 2015)*
- ***Privacy Data & Confidential Information theft* is the top concern** – even US government fell into victim to Chinese hackers
- **Different business segments will have different priorities and infrastructure for a compliance program**
  - Retail, financial, health care, telecommunication: customer/patient data
  - Manufacturing, BtoB businesses: confidential business information
  - New business model or software (such as Uber): could be both

Challenges Facing Multinational Companies

- Building a global privacy program
- Cross-border data transfer
- Data security
- Against the back drop of:
  - Increasing complexity of privacy laws regime
  - Regulatory discrepancies in different jurisdictions
  - Emerging of new business models
  - Evolving culture norms

DATA PRIVACY

Personal Data Legislation in Taiwan

Personal Information Protection Act of 2012

- Replaces the "Computer-processed Personal Data Protection Act," which is narrower in its scope of protection
- A general law regulating the collection, processing, use and disposal of personal data
- One of the most rigorous legislations in all jurisdictions (incorporated key elements from Directive 95/46/EC)
- Applies to both the public and private sectors
- Civil, criminal and administrative liabilities for violations
- Group litigation for civil damages led by NPOs available

Global Perspective (1/4)

- **Every jurisdiction where TSMC conducts business has laws of some sort to protect personal data.**
- **For the purpose of this presentation, we select six jurisdictions for analysis:**
  - China
  - Japan
  - Netherlands
  - Korea
  - Taiwan
  - United States

Global Perspective (2/4)

- **Except for the U.S. and China, each jurisdiction has a dedicated data protection law.**
  - U.S. system adopted a *sectorial approach* and has about 20 sector-specific data privacy/security laws and hundreds of state laws (where the (in)famous *breach notification obligation* thrives)
- **While the definition of personal data is generally consistent - data related to identified or identifiable natural person - the scope of "sensitive data" varies.**
  - Medical and criminal record, sexual preference and genetic information are typical sensitive information.
  - Race, religious belief, political opinion are not necessary deemed "sensitive" by every jurisdictions.
- **Netherlands and Korea have a dedicated personal data protection agency**
- **Korean law mandates a designated data protection officer for every data processor**

Global Perspective (3/4)

- **Requirements For Data Collecting And Processing:**
  - Processing personal data must be for a specific and legitimate purpose, and the data subject should be notified in advance
  - Explicit consent is required for processing sensitive data (unless the collecting of such data is specifically authorized by law)
  - Use of personal data should be within the scope of the original purpose used to collect the data
- **Onward Transfers:**
  - To any third party: "Notice and Choice Principle" applies
  - Netherlands follows the EU Directive which permits cross-boarder transfer only when the receiving country provides "adequate" privacy protections.

  Problem: U.S. regime is not deemed as offering adequate protection, so U.S. companies must rely on the *safe harbor program* and be separately certified by the EU as meeting EU requirements.
- **Security Measures:** Reasonable technical, physical and organizational measures to ensure data safety is a global requirement

Global Perspective (4/4)

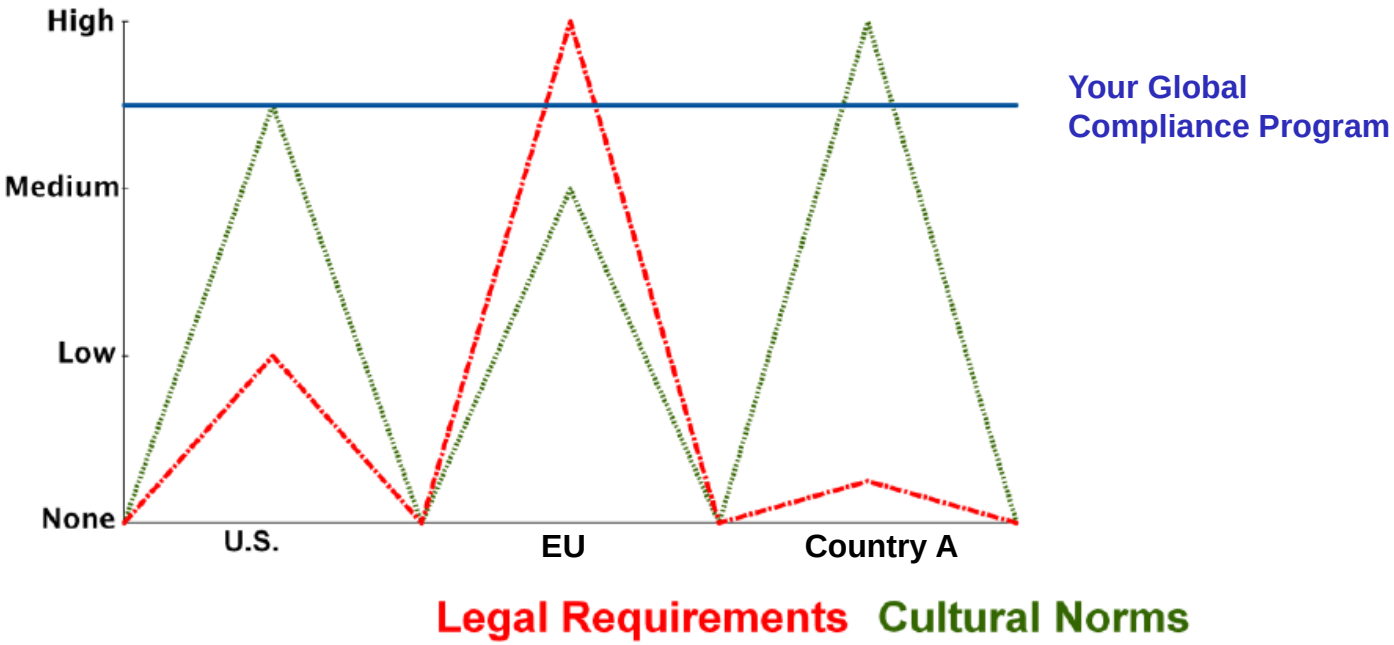
- **Breach Notification – Obligations to notify the regulator or individuals of breaches of security**
  - A *big thing* in the U.S.
    - Required by 46 of 50 states, NYC, Washington DC, and many Federal laws
    - The notice must reasonably describe the incident, the data at issue, and what the data owner has done to mitigate any harm and reduce the prospects for a repeat event
  - Netherlands/EU: No such requirement yet, but it is mandated by the pending EU Data Protection Regulation (published on Jan. 25, 2012)
  - Other jurisdictions: Either a legal requirement or a recommendation in governmental guidelines.
- **Penalties for Violation:** In jurisdictions where a dedicated law is available, both criminal and civil liabilities (including administrative fine) may be imposed

So we know coping with global privacy regulations is a complex issue.

Now What?

Building A Compliance Program

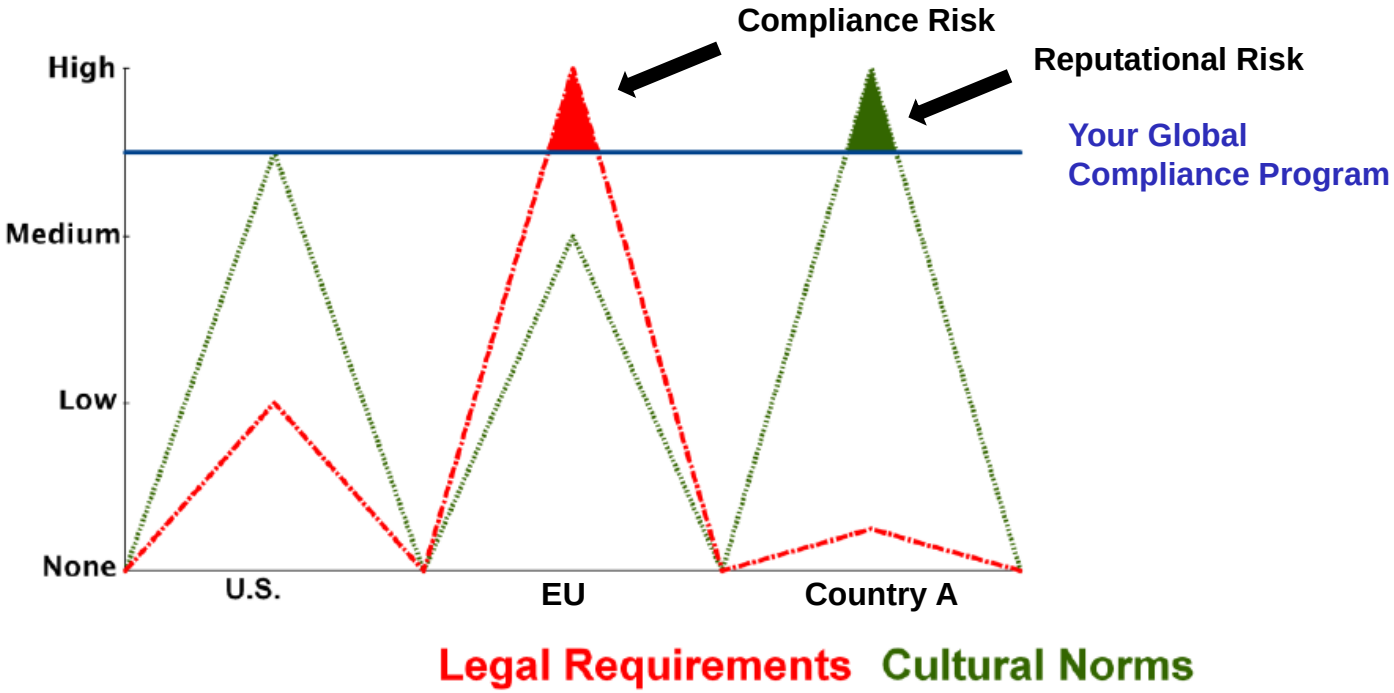
Balancing the risk of incompliance and practicality



From: Gartner, Technical Insights: Road Maps for Managing Multinational Privacy Risks, 2012

Building A Compliance Program

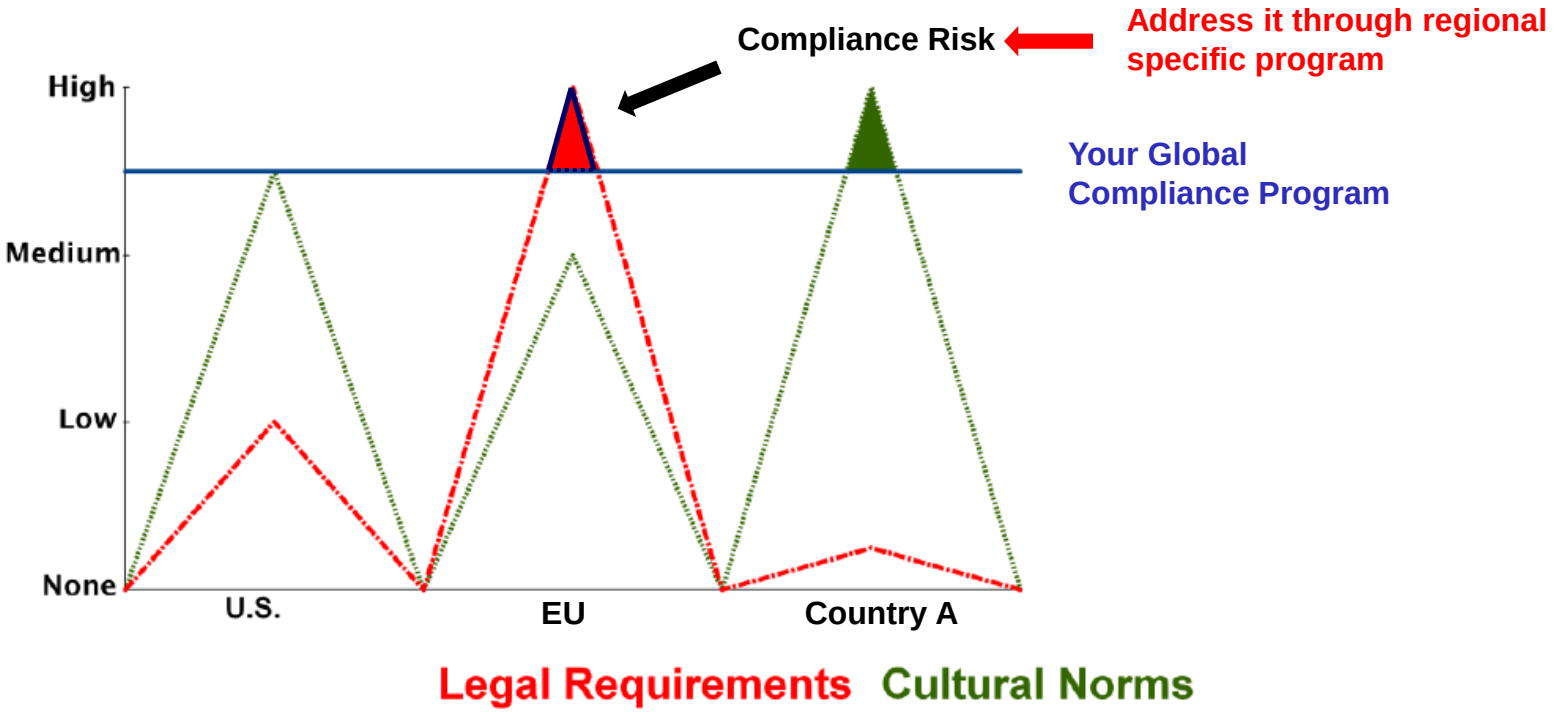
Balancing the risk of incompliance and practicality



From: Gartner, Technical Insights: Road Maps for Managing Multinational Privacy Risks, 2012

Building A Compliance Program

Balancing the risk of incompliance and practicality



From: Gartner, Technical Insights: Road Maps for Managing Multinational Privacy Risks, 2012

DATA SECURITY

Data Security

- **Recent cases show that dealing with a data security breach is not only painful but costly**
- **Home Depot:** data breach involved leakage of consumers' private information (including up to 56 million credit/debit card numbers)
  - Costs were $63M in 2014.
  - Has been hit by litigation from consumers and financial institutions
  - Cost another $7M in 1Q2015.
- **Others:** JPMorgan Chase & Co., Anthem Inc., Sony Pictures Entertainment Inc., Target Corp., and the US Government
  - Target's breach is considered one of the largest hacks in U.S. history

“These data breaches are only the most visible fights on a vast battlefield of digital espionage.”

The Atlantic, June 4, 2015

Compliance Tips

- **Be clear and open with individuals about the purpose of the collection and how their personal data will be used.**
- **Process data consistent with your notice.**
- **Destroy or anonymize data that is no longer needed.**
- **Develop a global compliance program that makes sense to your business model and the regions your business operates.**
- **Consult the Legal Department whenever:**
  (1) Sensitive data is collected or processed;
  (2) Collected data will be used for a new purpose
- **Notify the General Counsel immediately if a breach of security is suspected or discovered.**