Privacy in Asia: Building on the APEC Privacy Principles

Nir Kshetri

University of North Carolina—Greensboro

Workshop 28 , September 4, 2013 APrIGF

Current framework for protecting privacy online in the U.S.

- Reliance on self-regulation
- Sarbanes–Oxley (SOX) Act: . Accuracy of financial data
  - IT controls to ensure that data are accurate and are protected from unauthorized changes.
- Health and Human Services Health Insurance Portability and Accountability Act (HIPAA): technical, physical and administrative security measures to protect the privacy, integrity, and availability of patients' data
  - Failure to comply: up to $250,000 in fines and up to 10 years in prison

China, EU, and the US approaches to privacy

	China	EU	The U.S.
Salient feature	Encouraging purely economic use of ICTs and strict cyber-control measures	Strict enforcement of privacy rights through legislation	Preference to rely mostly on voluntary self-regulation but has sector-specific regulations for sensitive data.
Key driving factors	Need of balancing economic modernization and maintenance of unity and stability through political control.	World War II-era fascists' and post-War Communists: Europeans are more fearful of the prospect of the abuse of personal information.	Encouraging marketing and innovations.
Effects on IT providers	Lack of specificity required for accurate understanding and compliance: the 2012 Online Data Protection Regulation is broad, vague and like guiding principles rather than a law. Many provisions such as department/agency to supervise/enforce are unclear.	Strict regulations and the lack of economies of scale: inefficiencies and acted as a barrier to incentive for the development and diffusion of the cloud and other technologies.	There is a fear among some EU-based consumers and activists that U.S. cloud service providers are required to disclose data stored in clouds to their government without the data owner's consent or knowledge.
Effects on IT users	Unavailability of some services has been a concern. Some foreign firms have located their servers in neighboring countries, which has caused a severe negative impact on the quality of services.	Enjoy high level of privacy but due primarily to the lack of choice and quality of cloud services, consumers are slower to adopt the cloud.	There have been some concerns related to the government's monitoring and companies' misuse of citizens' information.

Key stakeholders in privacy discussion: Special interest groups and the private sector

- **U.S.:** The American Civil Liberties Union (ACLU), The Electronic Privacy Information Center (EPIC), The Electronic Frontier Foundation (EFF), and Others: Urged DHS to Stop Creation of National Identity System
- **Europe:**
  - ETNO: lobbied for an international privacy standard, simplification of rules governing data transfers, and others—expected to enable European companies to compete with those in the U.S.
  - Oracle, Cisco, SAP, Apple, Google and Microsoft: lobbied to streamline EU's fragmented national data protection laws.
  - Jan. 2011: Microsoft general counsel, spoke to the French National Assembly
- **India:** NASSCOM
- **China:** ISC

Thank you!