International Data Privacy: EU and APEC

Andrea L. Charters

Vice President & Associate General Counsel

Interest in international data privacy

- Both customer accounts and Human Resources records are subject to privacy and data security regulation
- Credit card data is especially important, especially if stored for renewals
- VoIP connections for online products pose additional concerns for government regulation and supervision of sites

Overview of the Comparative Laws

- EU led the data privacy and security movement
- US is working through APEC to establish alternative data privacy standards
- APEC refers to Asia-Pacific Economic Cooperation
- Operating in, and even selling to residents located in, other national jurisdictions requires an evaluation of data privacy law

Question for Audience

- Do you sell internationally at retail?
  - Yes
  - No

Question for Audience

- Have you filed with the US Department of Commerce for the US – EU Data Transfer Safe Harbor?
  - Yes
  - No

Question for Audience

- Have you considered establishing an APEC compliance program?
  - Yes
  - No

EU vs. APEC

EU	APEC
EU Led	US Led
In-house audit	Audit verified by outside party
Built off EU Directive and implementing national laws	Built off APEC agreement led by US
Certification from US DOC to obtain Safe Harbor for Data Transfer from EU	No concept of “adequacy” – substitutes objective measures
Review of contracts and data security	Review of 51 questions: formalize info
Review of law, contracts and security	TRUSTe or another auditor
Both customer and employee data	Both customer and employee data
Safe Harbor for transfers from EU to US	Covers multilateral data transfers
Privacy Policy on website is key	Privacy Policy on website is key
Implementation through US DOC and arbitration	Implementation through TRUSTe, DOC and outside auditors

History

EU	APEC
WWII legacy prompted strong concern about personal privacy, which influenced the computer age	Civil liberties concern for free speech has been a countervailing tide to privacy concerns
OECD 1980 Principles were the foundation of the EU privacy laws	OECD Principles are reflected in the APEC Privacy Principles
1981 Council of Europe action, followed by European Directive effective 1998, accompanied by Safe Harbor for transfers to US	Privacy law developed for banking, health and online privacy as a federal and state patchwork
Implementation by member states	Currently, efforts to have unified federal preemption of state laws
2011 EU Regulations under consideration	2011 – 2012 APEC Framework will be implemented
1998 Safe Harbor for data transfer to the US	APEC covers data transfers among signatory economies

Comparison of Key Terminology

EU	APEC
Personal data – info that can identify a natural person, such as name, address, credit card number	Personal information – also applies to natural persons
Data controller – party responsible for compliance with law on protection of personal data	Personal information controller
Data processor – party that can manipulate data, either on behalf of a data controller or the data controller itself	Personal information processors third parties
Sensitive information – health, union membership, political views	
Jurisdiction – any processing of data from users located in EU countries	Refers to “economies” – the participating jurisdictions – for sourcing the data

Principles

EU	APEC
	Preventing Harm
Notice – Privacy Policy	Notice – Privacy Policy; Q 1-4
Purpose – Privacy Policy	Collection Limitation, Use – Q 5-13
Consent – opt-in increasingly required; browser settings not sufficient under UK Cookie law to be effective 5/2012	Choice – Q 14-20; no prohibition on cookies
Security – corporate policies and IT	Integrity, Security – Q 21-35
Disclosure – Privacy Policy	Privacy Policy
Access – data subjects may request changes in their data; Privacy Policy	Access and Correction – Q 36-38
Accountability – if use Safe Harbor, must have a dispute resolution mechanism	Accountability – Q 39-51

Advantages of US - EU Safe Harbor

- Does not suggest a requirement of spot checking
- Can rely on yearly check of contracts
- Approved in 1-2 Business Days
- Does not require audit of third party performance – review of contracts suffices
- Does not require an outside audit, which will cost external resources
- Safe harbor covers compliance with national laws

Advantages of APEC Compliance

- Does not require dispute resolution through an arbitrator or data protection authority of another country
- Provides a higher level of bright line protection for participants
- Covers countries outside of EU
- Expanding list of participating countries
- Framework for structuring compliance with national laws

Question for Audience

- Have you evaluated the internal and external costs of APEC compliance, beyond what you have already done to comply with the EU-US Safe Harbor?
  - Yes
  - No

Question for Audience

- Have you considered complying with foreign domestic law privacy certifications, such as for Japan?
  - Yes
  - No

World Wide Effort

- We reviewed the laws of approximately 100 countries, many of which follow the EU and others of which have less clear laws
- To gain the best international practices, I recommend also using the APEC framework, which will be a relatively small additional expenditure of time and effort beyond that needed for the US – EU Safe Harbor

“Economies” Participating in APEC

Australia	New Zealand
Brunei Darussalam	Papua New Guinea
Canada	Peru
Chile	Philippines
People’s Republic of China	Russia
Hong Kong, China	Singapore
Indonesia	Chinese Taipei
Japan	Thailand
Republic of Korea	United States
Malaysia	Viet Nam
Mexico	

Ongoing Data Security Improvements

- Policies for data security: Compliance with the US – EU Safe Harbor and the APEC Principles also requires compliant data security
- These policies are continually updated and company compliance needs to be internally reviewed and certified
- Outside consultants also play a role in policing compliance at some companies

EU is Revising the Directive: Possible "Regulation"

- EU is considering issuing a "regulation" of specific rules instead of a "directive" subject to national laws in order to better harmonize the data privacy law

APEC

- Answers to 51 questions will need to be prepared
- TRUSTe certification will need to be obtained
- Time Horizon: expect to receive protection from this process no sooner than late 2011 or in 2012
- APEC offers the promise of simplifying and clarifying compliance with privacy requirements, which would substantially improve risk management

Conclusion

- International Data Privacy and Security law is a growth area
- Efforts to harmonize the law through safe harbors and international accords will make compliance more economical
- The burden remains on companies to improve their contracts with third parties, do due diligence on compliance by third parties, update their Privacy Policies and continually review data security

The views expressed herein are solely my own and represent neither legal advice nor the views of Rosetta Stone Inc.

- Special thanks go to Damon Greer and Joshua Harris of the Office of Technology and Electronic Commerce of the U.S. Department of Commerce for discussing with me the ongoing EU and APEC privacy initiatives, respectively, and to Terry McQuay of Nymity for discussing ongoing developments and providing a trial of access to the Nymity privacy database.