INTERNATIONAL
TRADE
ADMINISTRATION

The U.S. Privacy Framework & International Interoperability

Caitlin Fennessy
Office of Technology and E-Commerce
U.S. International Trade Administration

2012

Overview

- The U.S. Privacy Framework
- The White House Privacy Blueprint
- Enforceable Privacy Codes of Conduct
- Building International Interoperability

The U.S. Privacy Framework

Fourth Amendment to the U.S. Constitution

- Forms the foundation for privacy in the United States

- "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated"

The U.S. Privacy Framework

Commercial Privacy Protections

- Sectoral Privacy Laws – health, finance, education, children
- Tort Law – "right to be let alone"
- Voluntary Enforceable Codes of Conduct – enforced by U.S. Federal Trade Commission
- Company Privacy Programs – privacy policies and chief privacy officers

Public Sector Privacy Protections

- U.S. Privacy Act – covers government use of personal data

White House Privacy Blueprint

Released February 23, 2012

I. A Consumer Privacy Bill of Rights

II. A Multistakeholder Process to Develop Enforceable Privacy Codes of Conduct

III. Building on the FTC's Enforcement Expertise

IV. Promoting International Interoperability

White House Privacy Blueprint

Consumer Privacy Bill of Rights

I. Individual Control

II. Transparency

III. Respect for Context

IV. Security

V. Access and Accuracy

VI. Focused Collection

VII. Accountability

White House Privacy Blueprint

Multistakeholder Code Development

- NTIA is convening stakeholders to develop codes specifying how the Consumer Privacy Bill of Rights applies in specific business contexts
- The first multistakeholder process is focused on mobile application transparency
- Discussions are open to all interested stakeholders, transparent, and consensus-driven
- Code adoption will be voluntary, but once adopted fully enforceable by the U.S. Federal Trade Commission (FTC)

White House Privacy Blueprint

FTC's Enforcement Expertise

Privacy Blueprint

- Administration encourages Congress to give the FTC (and State Attorneys General) authority to enforce the Consumer Privacy Bill of Rights

FTC Report

- Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers - Released on March 26, 2012
  - Privacy by design
  - Simplified consumer choice
  - Greater transparency

White House Privacy Blueprint

International Interoperability

- Increase global interoperability to reduce barriers to information flow
  - Mutual recognition
  - Multistakeholder-developed codes of conduct
  - Enforcement cooperation

- International engagement toward interoperability
  - OECD Guidelines on Privacy & Transborder Data Flows
  - U.S.-EU and U.S.-Swiss Safe Harbor Frameworks
  - APEC Cross Border Privacy Rules

Benefits of Enforceable Privacy Codes

- **Timeliness**: Often developed faster than gov. regulation providing protection sooner
- **Expertise**: Development by those most closely tied to the information practices
- **Adaptability**: Allows industry to react to technological changes
- **Market friendly**: Avoids barriers to commerce
- **Reach:** Can expand enforcement authority capabilities

Challenges of Enforceable Privacy Codes

- **Accountability:** challenge to ensure privacy is enhanced in practice, not just in theory
- **Participation**: Industry support and adherence is vital, but can be difficult to gain
- **Agreement:** industry, consumer, and government interests are not always aligned
- **Legitimacy**: perception that industry interest is maximizing data access

Building International Interoperability

OECD Privacy Guidelines

- Finalized in 1980 and only now undergoing their first revision
- Established a common set of fair information practice principles (FIPPs)
- Early recognition of the need for transborder data flows to enable international trade

Building International Interoperability

OECD Privacy Guidelines

I. Collection Limitation

II. Data Quality

III. Purpose Specification

IV. Use Limitation

V. Security Safeguards

VI. Openness

VII. Individual Participation

VIII. Accountability

Building International Interoperability

Safe Harbor Framework

- Code of conduct designed to meet requirements of the EU Data Protection Directive
- Based on Seven Privacy Principles
- Approved by European Commission in 2000
- Voluntary participation of over 3,500 companies
- Self-certified compliance to Commerce
- Enforced by the Federal Trade Commission

Building International Interoperability

Safe Harbor Framework

Compliance

Adjust policies & practices to comply with SH requirements

Verification

Conduct self-assessment or outside compliance review

Certification

Self-certify compliance to the Department of Commerce

Enforcement

Through dispute resolution mechanisms and FTC enforcement

Building International Interoperability

APEC Cross Border Privacy Rules (CBPRs)

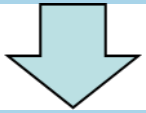
- The 21 APEC economies have multiple approaches to protecting the personal data collected in electronic transactions within their jurisdictions
- Compliance can be both confusing and costly
- APEC Privacy Framework developed in 2004
- APEC CBPRs were finalized and endorsed in 2011

Building International Interoperability

APEC Cross Border Privacy Rules

Join the Cross Border Privacy Enforcement Arrangement (CPEA)

Submit a letter of intent to participate in the CBPR System



Make use of at least one APEC-recognized Accountability Agent

Building International Interoperability

APEC Cross Border Privacy Rules

Building International Interoperability

APEC CBPRs: Realizing Benefits

- *Timeliness:* APEC proactively addresses current challenges to avoid future barriers
- *Adaptability:* Principles-based approach will allow organizations to tailor implementation
- *Expertise and Industry buy-in:* Industry has helped lead development of the CBPRs
- *Market friendly:* Initiated to overcome barriers to international trade
- *Reach:* Enforcement cooperation and Accountability Agents lend additional resources

Building International Interoperability

APEC CBPRs: Overcoming Challenges

- *Accountability:* CBPRs backed by certification, audits, and enforcement bolsters protection
- *Legitimacy:* Adoption of APEC principles into industry practices demonstrates commitment
- *Participation:* 16 companies across five countries participated in the test pilot
- *Agreement:* Continued commitment from economies helps address disagreements

Building International Interoperability

APEC CBPRs: How to Learn More

Attend a meeting of the APEC Electronic Commerce Steering Group as a guest observer

The next meeting will occur on in early 2012 in Jakarta, Indonesia

To apply for guest status
or for further information on APEC CBPRs,
contact Joshua Harris
Joshua.Harris@trade.gov

Conclusion

- What are Key Elements of Strong, Innovation Enabling Privacy Protection?

- What Elements Further Interoperability Between Data Protection Frameworks?

Thank you.

Caitlin Fennessy
Office of Technology and E-Commerce
U.S. International Trade Administration
Caitlin.Fennessy@trade.gov