



The United States Federal Trade Commission (FTC), along with co-organizers APEC and OECD, will hold an international conference on March 16-17, 2009 on the trans-border aspects of data security. This conference, first discussed at an OECD brainstorming session to identify

In one case, a European company makes a lawful transfer of personal data to the US. In another case, a US company outsources processing of data to another country. How do companies approach data security in these instances? How are inter- and intra-company transfers treated differently, if at all?

Part 2: At some point in the process in both cases, there is a data leak. As in many instances, it cannot be precisely determined when and where the data was lost. To what extent does the level of sensitivity of the leaked data have an impact? Which laws apply, and which country/ies can pursue an investigation? How can authorities collaborate?

MARTIN ABRAMS, Executive Director, Centre for Information Policy Leadership

12:15-1:30 Lunch

1:30-3:00 **Session 3: Data Security Practices in Industry**

While the law sets a bar for security, industry must implement it in a practical way. In the U.S., for example, the FTC requires a “reasonable” level of security through the FTC Act and the Safeguards Rule, and what is reasonable depends on the type of information held, the size of the business, and other factors. Other countries take different approaches. What is state of the art within industry? How do developers of data security tools stay current? And what can the regulators learn from industry?

MAUREEN COONEY, Chief Privacy Officer and Vice President for Public Policy, TRUSTe

DAVID HOFFMAN, Group Counsel for Global E-Business and Privacy, Intel Corporation

STEPHEN SCHARF, Senior Vice President and Global Chief Information Security Officer, Experian Inc.

LEIGH WILLIAMS, President, BITS, a division of The Financial Services Roundtable

Moderator: MOLLY CRAWFORD, Division of Privacy and Identity Protection, FTC

3:00-3:15 Break

3:15-5:00 **Session 4: Data Breach and Response Best Practices**

How do organizations respond to data breaches? And how should they? A number of countries are considering adopting data breach notification legislation, following the lead of the most of the US states. Has notification been good for consumers, and has it raised the priority for data security within companies?

DAY 2 — MARCH 17, 2009

8:45-9:00 **Keynote:** Commissioner PAMELA JONES HARBOUR, FTC

9:15-10:30 **Session 5: Data Flows and Cross-Border Conflicts**

Organizations moving data across borders often face difficult, sometimes inconsistent compliance obligations. Many organizations are seeking a solution to the problem, working to create systems that allow data transfer internationally under a single standard that protects consumers without unduly hindering the global information economy. There are clear challenges to finding consensus approaches in this area, but data security does appear to be one of the core elements around which common approaches can be more easily developed. What are the most promising approaches to addressing cross-border conflicts? What roles are foreseen for the various international organizations in addressing the challenges?

RICHARD BOURASSA, Chair, ECSG, APEC and Director, International Policy, Industry Canada

BILLY HAWKES, Data Protection Commissioner, Ireland

JANE HORVATH, Senior Privacy Counsel, Google

KRISTIN LOVEJOY, Director, IBM Governance & Risk Management strategy

MARC ROTENBERG, Executive Director, Electronic Privacy Information Center (EPIC)

HENRIETTS "JETTY" TIELEMANS, Partner, Covington and Burling LLP

Moderator: MICHAEL DONOHUE, Administrator, Privacy and Information Security, OECD

10:30-10:45 Be7t-dJ207L-pg-LSpan #M0004f/TT100T1011 1807004f/5100T10310312005/TT1 1 Tf11 0 0 11 28299.