RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Economic Impact of PRISM on Cloud Services & Safe Harbor

SESSION ID: TRND-R04A

Craig Spiezle

Executive Director & President,
Online Trust Alliance
https://otalliance.org

Challenges & Risks

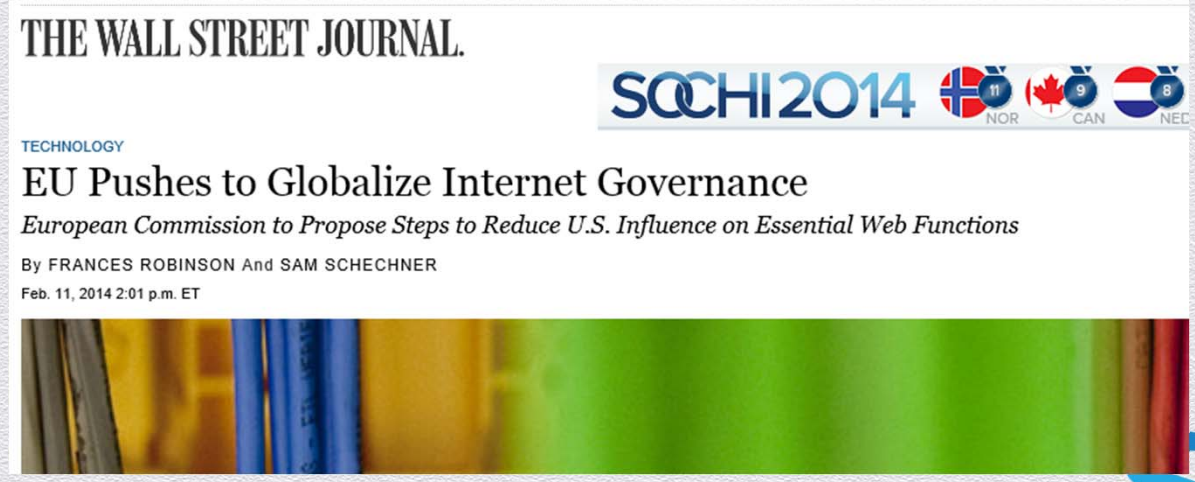
- Privacy Balkanization / Firewalling
- Privacy as a civil liberty is under threat
- Competitive disadvantages for US companies
- Decrease consumer trust in the digital economy
- Elongated and prolonged contract process
- Digital Trade Policy
- European Union Policies

Balkanization

- Process of fragmentation or division of a region or state into smaller regions or states that non-cooperative with one another.
  - Driven by perceived conflict between security and privacy interests and policy of public and private sectors.

Cascading Impact

The EU's executive body is raising pressure to reduce U.S. influence on the Internet, after revelations of widespread U.S. surveillance activities have caused what it calls a "loss of confidence".



THE WALL STREET JOURNAL.

SOCHI 2014

TECHNOLOGY

EU Pushes to Globalize Internet Governance

European Commission to Propose Steps to Reduce U.S. Influence on Essential Web Functions

By FRANCES ROBINSON And SAM SCHECHNER

Feb. 11, 2014 2:01 p.m. ET

Privacy Trade Barriers

News › World news › NSA

Fears over NSA surveillance revelations endanger US cloud computing industry

Companies say they could lose billions as customers become wary about their data being turned over to US authorities

Follow @dankaps

July 29, 2013

Overseas companies reluctant to use U.S. cloud after Snowden NSA leaks

More than half of the respondents polled in a recent survey said they would be "less likely" to

The U.S. cloud computing industry stands to lose $22 to $35 billion over the next three years as a result of the recent revelations about the NSA's electronic surveillance programs.

German DPAs Halt Data Transfer Approvals and Consider Suspending Transfers Based on Safe Harbor, EU Model Clauses

POSTED ON JULY 25, 2013 BY HUNTON & WILLIAMS LLP

On July 24, 2013, the Conference of the German Data Protection Commissioners at both the Federal and State levels issued a press release stating that surveillance activities by foreign intelligence and security agencies threaten international data traffic between Germany and countries outside the EEA.

USA TODAY SEARCH

NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION 50° SUBSCRIBE

Why Google could start a trade war over Europe's privacy rules

Timothy J. Toohey, Special for USA TODAY 3:01 p.m. EDT March 22, 2013

OTA Online Trust Alliance

#RSAC

RSACONFERENCE2014

Why Care?

- Growth is threatened by rising digital protectionism by several of our trading partners. It is imperative that the U.S. fight for strong rules to ensure businesses have the freedom to compete and innovate all around the world." Sens. John Thune, R-S.D
- "Trade in digital goods and services is growing and driving economic growth and job creation …. but outdated trade rules threaten this growth by providing opportunities for protectionist policies overseas," Sen Wyden OR

The Importance of Trans-Atlantic Trade

The US and EU continue to be each other's largest trading partners:

- Responsible for $5.3 trillion in commercial sales, 15 million jobs

A Significant Factor in Global Trade

- 41% of Global Purchasing Power
- The EU also represents 500 million potential consumers
- Cloud services have contributed to 21% of the GDP growth in mature economies over the prior five-year period.

Impact

- Fostering the growth of the Internet equals greater economic growth
- Conversely, threats to Internet can be viewed as an economic danger

Source: Transatlantic Economy 2013 (AmCham EU, Transatlantic Business Council &)

The Elephant In The Room – Safe Harbor

- Sparking a Robust Debate.
- Distinction between National Security and Commercial Privacy.
- EU Data Protection Directive recognized security exceptions.
- Safe Harbor was never designed or intended to address national security issues or government actions.
- Safe Harbor has been an easy target, but not the right target.

Safe Harbor Framework Background

- **U.S.-EU** & **US-Swiss Safe Harbor Framework** - effective in November 2000.
- Critical mechanism to bridge the gap between the U.S & EU
- Companies make a voluntary representation to comply.
- Allows companies to certify to 7 principles for data transfers: notice, choice, onward transfers, access, security, data integrity, enforcement.
- Member States can only stop transfers to individual organizations based on evidence that entity is violating Safe Harbor principles.
- The U.S. Department of Commerce & Federal Trade Commission are confident that Safe Harbor Framework is not going away

PRISM, the NSA & Safe Harbor

- The Safe Harbor addresses the commercial transfer of personal data, otherwise known as commercial data. PRISM, **involved government access, not transfer of commercial data**.
- Changes to government access would be covered by changes to the **Law Enforcement Directive,** being negotiated by the EU and US (not part of data protection reform).
- **Fallout** for US cloud companies doing business in the EU - restrictive EU "localization" requirements, protectionist tactics
- The EU Parliament's LIBE Committee (The Committee on Civil Liberties, Justice and Home Affairs) has called for **an end to the Safe Harbor** –to "protect" the privacy of EU citizens.

Rebuilding Trust in EU-US Data Flows

- Statement by European Commission on President Obama's remarks on the review of U.S. intelligence programs – Jan 17, 2014
  - A number of questions still remain open and will need to be addressed in detail. We will therefore continue our dialogue with the U.S., along the lines set in the Commission's communication of 27 November 2013 on "Rebuilding Trust in EU-US Data Flows", which includes, in particular:
  - An improvement of the Safe Harbour scheme that would address security issues in a way that strengthens trust in transatlantic data transfers to the U.S. in the commercial sector.
  - The swift conclusion of an umbrella agreement on data protection in the area of law enforcement that will guarantee enforceable rights for EU citizens, including judicial redress for EU citizens not resident in the U.S..

EU Recommendations – December 2013

- EU report criticized and published **Recommendations**:
  - Self Certified Companies should publicly disclose their privacy practices, include a link to DOC website, and publish contract conditions with sub-contractors.
  - Provide link to Alternative Dispute Resolution provider; ADR should be easily “readily available and affordable”.
  - **Disclose law enforcement access to data and use the national security exception only when “strictly necessary & proportionate.”**
  - Commerce should maintain list of participants, monitor complaint reporting and actively investigate false claims of adherence.

Digital Trade Barriers & Fall Out

- Locate data centers in-country as a condition of market access,
- Mandating that companies must store and process data locally
- Impact of cutting off cross-border data flows
- Risk of precluding the provision of Web-based services

Last updated: January 22, 2014 10:26 pm

Microsoft to shield foreign users' data

By James Fontanella-Khan in Brussels and Richard Waters in San Francisco

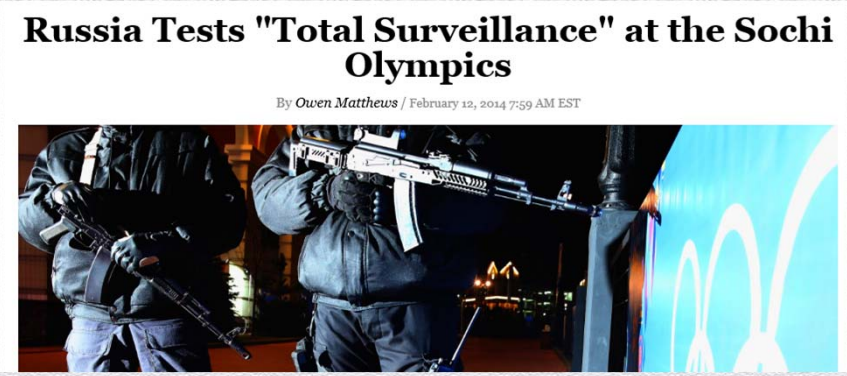
Microsoft will allow foreign customers to have their personal data stored on servers outside the US, breaking ranks with other big technology groups that until now have shown a united front in response to the

Microsoft to Let Foreign Customers to Store Data Overseas

By Dina Bass and Ian King | Jan 23, 2014 10:03 AM PT | 2 Comments | Email | Print

Reality?

System of Operative-Investigative Measures (SORM)



Russia Tests "Total Surveillance" at the Sochi Olympics

By *Owen Matthews* / February 12, 2014 7:59 AM EST

- SORM makes PRISM system look distinctly underpowered.
- State-of-the-art ability to perform real-time 'deep-packet-inspection' - reading and listening to communications and setting off alarms when triggered by specific keywords.

Source: http://mag.newsweek.com/2014/02/14/russia-tests-total-surveillance-sochi-olympics.html

Citizens Must Demand

- That the government and businesses follow the law
- The law is robust and protects civil liberties
- The government foes not circumvent industry standards of info security solutions
- We have transparency, accountability and control in both government and business.

Resources

- Online Trust Alliance https://otalliance.org
- U.S Department of Commerce Safe Harbor http://export.gov/safeharbor/index.asp
- EU Parliament's LIBE Committee http://www.europarl.europa.eu/committees/en/LIBE/home.html
- TRUSTe Safe Harbor Program http://www.truste.com/products-and-services/enterprise-privacy/eu-safe-harbor-seal
- EU Statement on National Security Issues http://europa.eu/rapid/press-release_MEMO-14-30_en.htm
- Transatlantic Economy http://transatlantic.sais-jhu.edu/publications/books/Transatlantic_Economy_2013/TE2013%20volume%201.pdf
- Rebuilding Trust In US Data Flows http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf