Separated By A Common Goal

Emerging EU and US Information Security Law: Allies or Adversaries?

Bryan Cunningham, Principal, Morgan & Cunningham LLC
Amanda Hubbard, Fulbright Scholar

Standard Legal Disclaimer (sortof)

(in very small print, of course)

You have the right to remain silent. Should you give up that right, anything you say may be used against you, now, or in a subsequent presentation.

The information presented is accurate as of the day of the presentation, but could change tomorrow (and in some cases we hope it does). Please take steps with your legal counsel to verify the applicability to you of laws and regulations before proceeding with any course of action described today.

None of the information provided should be considered legal advice. Each situation has unique facts and applicable regulations that require the services of a legal advisor trained and licensed to practice law in your jurisdiction. If you want our advice on US information security law or best practices, you'll have to hire us. If you need an EU lawyer, you'll have to find someone licensed in your country.

The opinions and perspectives of each of the speakers are personal views and do not reflect the official opinions of any government organization, private research institution, private company, international conspiracy, etc. We are both bold, innovative, opinionated, and stubborn all on our own. All names have been changed to protect the stupid and guilty. Any resemblance to persons you know, or think you know, or once knew is purely your overactive imagination.

Warning: sleeping hazard (if we catch you sleeping, we will bring you up and make you part of the examples); do not use power tools while attending the presentation; please don't try this at home; use only under adult supervision; do not remove tags before leaving the store; don't run with scissors; life vests are not located under your seats so don't look for them; emergency exits are located in convenient locations around the room; mix thoroughly with alcohol after prolonged exposure, and, of course, keep arms and legs inside until the ride has come to a complete stop.

Introduction: Security & Privacy are Not Mutually Exclusive

Courts and legislatures on both sides of the Atlantic recognize the balance between the two interests

Example: Charter of Fundamental Rights of the European Union, “Chapter II Freedoms”

Article 6 Right to liberty and security: Everyone has the right to liberty and security of person

Article 7 Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications

BUT…What do these words mean???

Introduction: What is "Privacy"?

- Privacy is "the right to be left alone."
  - *U.S. Supreme Court Justice Louis Brandeis, 1928*
- Privacy is "[t]he right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information."
  - Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO, at 7.
- "You Have Zero Privacy. Get over it."
  - *Sun Microsystems CEO Scott McNealy, 1999*

Introduction: What is “Privacy”?

Is “privacy” today more about the initial *collection* of information about us, OR controlling the *uses* of information collected about us?

Introduction: What is “Security”?

Security • noun (pl. securities)

1 the state of being or feeling secure.

2 the safety of a state or organization against criminal activity such as terrorism or espionage.

3 a thing deposited or pledged as a guarantee of the fulfillment of an undertaking or the repayment of a loan, to be forfeited in case of default.

4 a certificate attesting credit, the ownership of stocks or bonds, etc.

– Oxford English Compact Dictionary

Security & Privacy are neither static concepts nor mutually exclusive

- Governments *and the private sector* should work toward:
  - Better accountability for *collecting* information;
  - Better rules for *using* information; and
  - Enhancing technology to protect *both* privacy of individuals and security of individuals, groups, and countries through, e.g:
    - Anonymization;
    - Identity management systems; and
    - Dynamic permissioning and escalating thresholds and approvals for access and use

Agenda:

I. Changes in Technology necessitating legal change
II. How resulting laws affect balance between security and privacy
III. How do changes affect security industry (and you)?
IV. Current areas of debate and how to participate

Agenda:

I. **Changes in Technology necessitating legal change**

II. How resulting laws affect balance between security and privacy

III. How do changes affect security industry (and you)?

IV. Current areas of debate and how to participate

I. Changes in Technology necessitating legal change

- **Fact:** Legal changes will never keep pace with technology development
- **Why?**

  Globalization vs. Jurisdiction

  Convergence vs. Divergence

  Bandwidth vs. Bandwagons

I. Changes in Technology necessitating legal change

Globalization

- International telecom mergers
- Global services like VOIP (e.g. Skype-in)
- Innovation faster than legislation
- Off-site storage in multiple countries

Jurisdiction

- National laws have geographic limits (at least in practice)
- International treaties subject to national level implementation
- Questions of standing to challenge laws in other countries

I. Changes in Technology necessitating legal change

Convergence

- Satellite transmission of mixed media
- Wired and wireless world changing and overlapping

Divergence

- Regulations based on data storage format
- Antique property laws based on concept of “publishing” or “control”
- Laws based on technical data versus content (e.g. what is an IP address?)

I. Changes in Technology necessitating legal change

Bandwidth

- Greater capacity means greater responsibility -- on the parts of users, providers, and governments

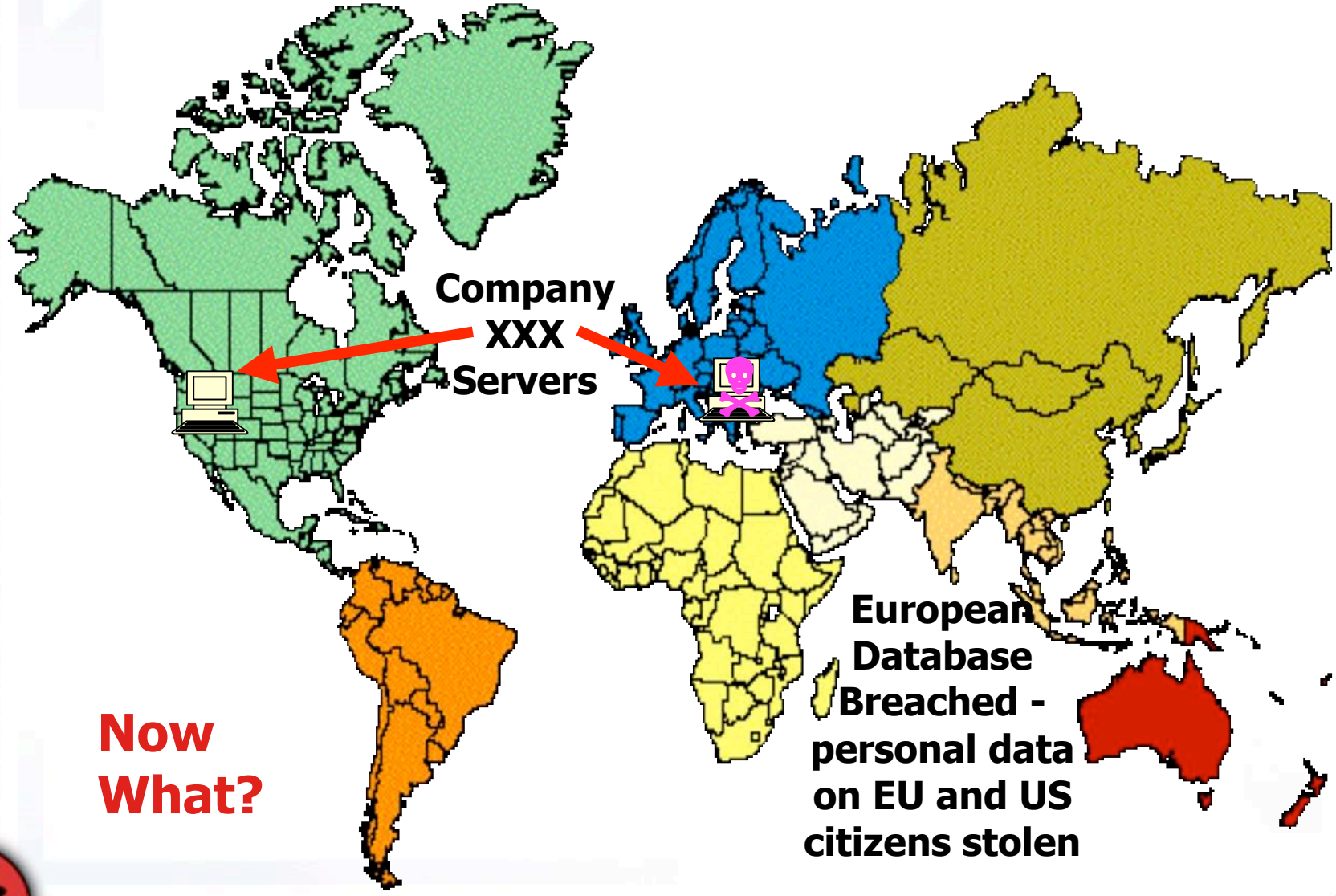
Bandwagons

- Political soundbites too often based on polls or media coverage, rather than facts, law, and technological realities

Fair Warning: Pop Quiz Next

- *Coming Next:* Survey of laws on both sides of the Atlantic shortly and then give you tips on what you can do to comply or try to change the laws
- More fun to do the first Case Study “cold,” before doing the legal mumbo jumbo -- don’t worry, it won’t hurt -- much

Pop Quiz: Case Study



Pop Quiz: Lessons Learned

- *Have an incident response plan, including who to contact when a breach occurs*
- *Know the reporting requirements for every country where your data resides*
- *Consult counsel to help you properly balance your legal responsibilities*
- *Have a plan in place to weigh the costs and benefits of notifying victims and the public of the breach*
- *Even if you don't go public, have a plan for public relations when the breach becomes public - either through official notification or through a leak*

Agenda:

I. Changes in Technology necessitating legal change

II. How resulting laws affect balance between security and privacy

III. How do changes affect security industry (and you)?

IV. Current areas of debate and how to participate

II. How resulting laws affect balance between security and privacy

- Why are countries enacting new information security/privacy-related laws?
  - Improving public confidence in commerce and privacy protections;
  - Intense scrutiny in response to breaches;
  - International legal obligations;
  - Statistics are showing disturbing trends;
  - Recognition of national security implications; and
  - Need for rational frameworks for regulation/litigation

II. How resulting laws affect balance between security and privacy

United States

1. Breach disclosure laws (state and federal)
2. Unauthorized access/computer abuse
3. Financial information
4. Personal data
5. Health information
6. Information collection, use and sharing

II. How resulting laws affect balance between security and privacy

United States (cont.)

- Federal/state enforcement/consent decrees
  - Microsoft & Ziff Davis last *20 years*
- Contractual obligations
- Statements on your website
- Victims lawsuits
- Employee lawsuits
- Shareholder lawsuits

II. How resulting laws affect balance between security and privacy

United States (cont.)

- FISA and Other Electronic Surveillance
- USA PATRIOT Act
  - E-mail and “chat” monitoring
  - “Roving” wiretaps
  - Business Records/Admin. subpoenas
- Pattern/link analysis
- Credit reporting services and other “datamine owners”

II. How resulting laws affect balance between security and privacy

European Union

1. Privacy protection
2. Data preservation
3. Information sharing

II. How resulting laws affect balance between security and privacy

European Union - Sources of privacy protection

- EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- EU Directive 2002/58/EC (2002) on privacy and electronic communications
- EU Directive 97/66/EC (1997) on the processing of personal data and the protection of privacy in the telecommunications sector
- Treaty on the European Union (TEU): Article F
- European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR): Art. 8
- EU Charter of Fundamental Rights of 7 December 2000

II. How resulting laws affect balance between security and privacy

European Union -- Data preservation

- No EU Directive currently in place, though drafts are in progress;
- Commission has started working on the issue because of the differences between laws in member states:
  - Majority of EU member states have no mandatory data retention obligations;
  - Of those states that do have laws, implementation is still ineffective or incomplete;
  - Of those states with effective implementation, the periods, scope, and subject matter vary.

II. How resulting laws affect balance between security and privacy

European Union -- Information sharing

- Result of London and Madrid bombings
- Goal is better cooperation between law enforcement bodies
- No Directive yet in place
- Commission taking steps to draft provisions
- Not sure yet how non EU countries will be dealt with

II. How resulting laws affect balance between security and privacy

Is the balance shifting?

- Legislatures recognizing (slowly) old ways of regulating security/privacy no longer adequate
- Citizens paying closer attention to personal activities online

Which way is the balance shifting?

- Crystal ball time

Agenda:

I. Changes in Technology necessitating legal change

II. How resulting laws affect balance between security and privacy

III. How do changes affect security industry (and you)?

IV. Current areas of debate and how to participate

III. How do changes affect security industry (and you)?

Businesses have interests in securing network assets pursuant to legal requirements:

1. Protecting network resources;
2. Impacts of criminal investigation;
3. Impact of civil lawsuits;
4. Loss of IP;
5. Bad press;
6. Devaluation of company/shareholder suits; and
7. Mandatory disclosure to victims and public

III. How do changes affect security industry (and you)?

Businesses also have interests in creating strong security/privacy protection:

1. Protect own customer records;
2. Protect employees;
3. Comply with law;
4. Prevent costly breaches;
5. Avoid repercussions of reporting requirements; and
6. Do the "Right Thing".

III. How do changes affect security industry (and you)?

Murphy's corollary to Newton's Third Law*:

For every legal use of a technology, there are endless possibilities for illegal uses.

*as twisted by Cunningham and Hubbard

Pop Quiz: Case Study 2

Same Multinational Corporation has databases in two countries (EU Member State and US) and same breach of server in California and data about both EU and US customers stolen from a database … BUT

a. *Belgian law enforcement asks you not to disclose breach until they have secured critical evidence in order to arrest a suspect; AND*
b. *US and the European Server Location have conflicting disclosure requirements*

Now what do you do?

Pop Quiz: Lessons Learned

- *Know your rights and responsibilities when dealing with law enforcement*
- *Consult counsel to help you properly balance your legal responsibilities*
- *Work with LE to get them what they need, but minimize downtime of employees and information*
- *Be able to credibly explain later why you delayed notification (i.e., to assist the investigation)*

III. How do changes affect security industry (and you)?

- Current legislatures often do not have the time, experience, or technical expertise to craft laws both general and specific enough to address complex technical issues
- Private sector often better at complex technical regulatory issues

III. How do changes affect security industry (and you)?

Special interest groups are using money, power, and advocates to push the pendulum as far as possible in pending legislation, without adequately addressing technical challenges to proposed “solutions” or, in many cases, even recognizing changing technological realities:

1. Privacy groups;
2. Law Enforcement; and
3. Parties caught in the middle.

III. How do changes affect security industry (and you)?

Anticipating change allows for better business adaptation to the results of new legislation:

1. Time;
2. Personnel;
3. System resources;
4. Disclosure dilemmas; and
5. Multi-jurisdictional issues.

III. How do changes affect security industry (and you)?

***Seven Steps to Best Adapt to Changes*:**

1. **Know the current rules.** Why?
2. **Stay current on legal and policy debates.** Why?
3. **Hire knowledgeable outside legal counsel**, or train your in-house corporate attorney. Why?
4. **Have thorough, sensible response plans.** Why?
5. **Practice and review plans regularly.** Why?
6. **Frequently update plans and information security posture.** Why?
7. **Perform independent reviews periodically.** Why?

Agenda:

I. Changes in Technology necessitating legal change
II. How resulting laws affect balance between security and privacy
III. How do changes affect security industry (and you)?
IV. Current areas of debate and how to participate

IV. Current areas of debate and how to participate

United States

1. Privacy
2. Data preservation
3. Electronic surveillance
4. Access to information (including cross-border searches)
5. Sharing of information

IV. Current areas of debate and how to participate

European Union

1. Privacy
2. Data preservation
3. Electronic surveillance
4. Access to information (including cross-border searches)
5. Sharing of information

IV. Current areas of debate and how to participate

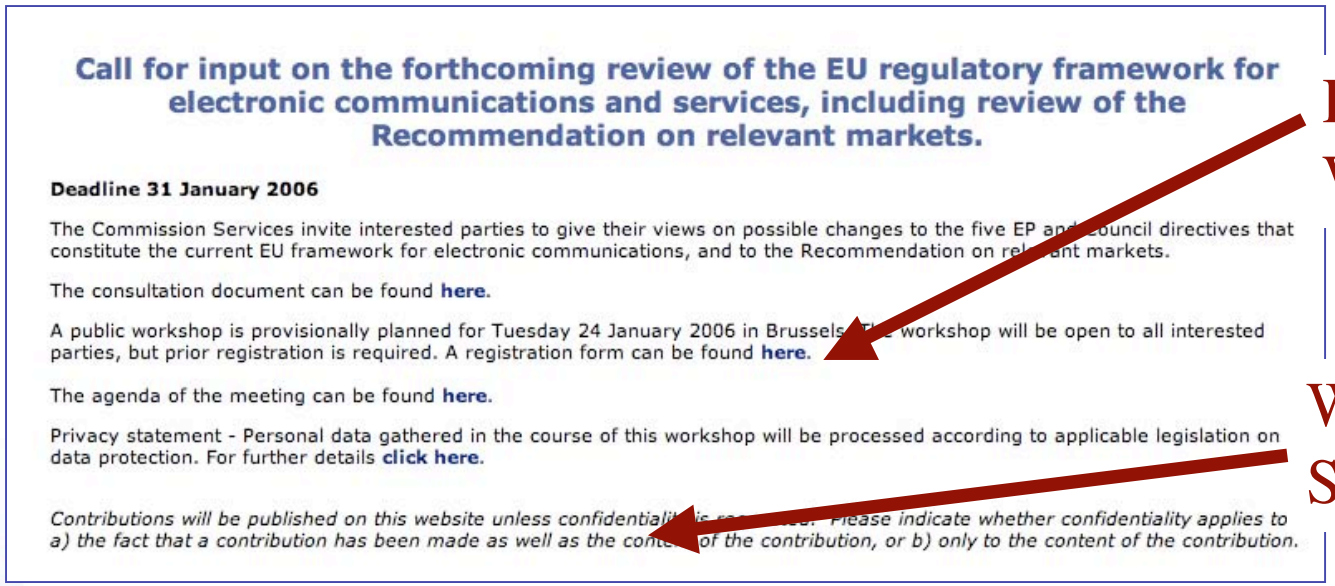
European Union Information Society Portal:
http://europa.eu.int/pol/infso/index_en.htm

Call for input on the forthcoming review of the EU regulatory framework for electronic communications and services.

IV. Current areas of debate and how to participate

European Union:

http://europa.eu.int/pol/infso/index_en.htm



Call for input on the forthcoming review of the EU regulatory framework for electronic communications and services, including review of the Recommendation on relevant markets.

Deadline 31 January 2006

The Commission Services invite interested parties to give their views on possible changes to the five EP and Council directives that constitute the current EU framework for electronic communications, and to the Recommendation on relevant markets.

The consultation document can be found **here**.

A public workshop is provisionally planned for Tuesday 24 January 2006 in Brussels. The workshop will be open to all interested parties, but prior registration is required. A registration form can be found **here**.

The agenda of the meeting can be found **here**.

Privacy statement - Personal data gathered in the course of this workshop will be processed according to applicable legislation on data protection. For further details **click here**.

Contributions will be published on this website unless confidentiality is requested. Please indicate whether confidentiality applies to a) the fact that a contribution has been made as well as the content of the contribution, or b) only to the content of the contribution.

Public Workshops

Written Submissions

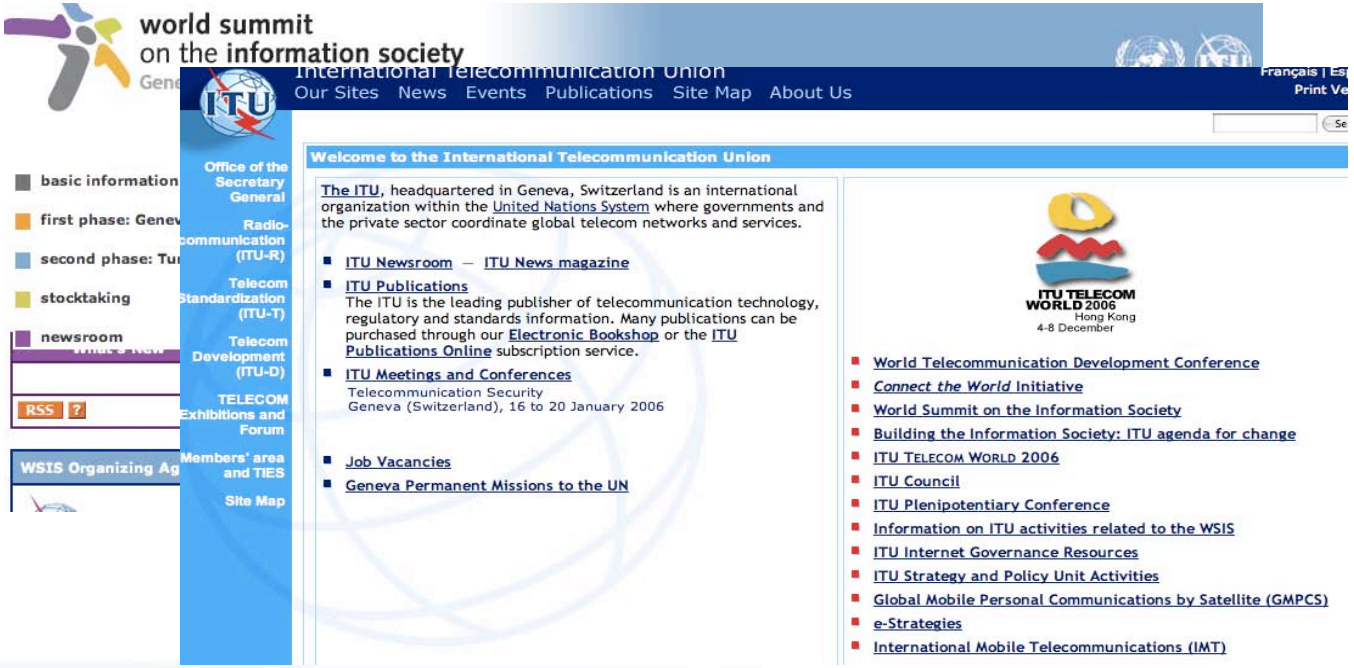
IV. Current areas of debate and how to participate

International Initiatives that could impact both Europe and the US

- UN Information Security Initiatives
- World Summit on the Information Society: 2006 Forum
- National Ratifications of the COE Cybercrime Convention

IV. Current areas of debate and how to participate

International Initiatives that could impact both Europe and the US:



IV. Current areas of debate and how to participate

For more information on the International Initiatives that could impact both Europe and the US:

- http://www.itu.int/wsis/implementation/index.html
- http://www.itu.int/home/index.html
- Also consider participating through private interest groups such as the International Chamber of Commerce www.iccwbo.org

Separated By A Common Goal- Summary

- The EU uses a comprehensive general regulation methodology
- The US has chosen a sector or subject-specific regulatory scheme
- Future changes in technology will require additional legal changes to maintain a balance between security and privacy
- You don't have to stand by and wait for results.
- You can take steps to influence the debate and protect your company

Separated By A Common Goal-

Emerging EU and US Information Security Law: Allies or Adversaries?

Bryan Cunningham

Principal

Morgan & Cunningham LLC

bc@morgancunningham.net

(+1) 303-743-0003

Amanda Hubbard

Fulbright Scholar

Norwegian Research Center for Computers and Law

Hubbard.a.m@gmail.com

(+47) 9366-5050