What Every In-House Counsel Needs to Know About Data Security and Privacy

How you can manage your company's obligations under federal and state data privacy and security laws

September 7, 2011

Colin J. Zick, Esq.
Foley Hoag LLP

Edward Palmieri, Esq.
Privacy Counsel, Facebook

Data Privacy and Security: Why Should It Be a Priority?

- *More federal and state laws, increasing penalties*
- *Theft of consumer information increasing, resulting in government investigations, private consumer litigation and harm to your brand:*
  - *Sony*
  - *TJX/Heartland*
- *Attacks on systems increasing:*
  - *State-sponsored attacks from China and North Korean and against Iran: "Google says Chinese hackers broke into Gmail"*
  - *NYSE has suffered several recent incursions*
- *Wikileaks*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Laws Impacting Data Privacy and Security

- *Federal and 50 State Laws Governing:*
  - *What information can be collected*
  - *How it must be stored and secured*
  - *Under what circumstances it can be shared*
  - *Under what circumstances it can be disclosed*
  - *Requirements for responding to data breaches and data losses*
  - *Penalties for data breaches and data losses*

- *And that's without taking into account the international laws . . .*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

List of U.S. Laws Impacting Data Privacy and Security

- *Administrative Procedure Act. (5 U.S.C. § § 551, 554-558)*
- *Cable Communications Policy Act (47 U.S.C. § 551)*
- *Cable TV Privacy Act of 1984 (47 U.S.C. § 551)*
- *Census Confidentiality Statute (13 U.S.C. § 9)*
- *Children's Online Privacy Protection Act of 1998 (15 U.S.C. § 6501, et seq., 16 C.F.R. § 312)*
- *Communications Assistance for Law Enforcement Act of 1994 (47 U.S.C. § 1001)*
- *Computer Fraud and Abuse Act, as amended by the USA PATRIOT Act (18 U.S.C. § 1030)*
- *Computer Security Act (40 U.S.C. § 1441)*
- *Consumer Financial Protection Act of 2010 (Pub. L. No. 111-203, 124 Stat. 1376)*
- *Criminal Justice Information Systems (42 U.S.C. § 3789g)*
- *Counterfeit Access Device and Computer Fraud Abuse Act of 1984 (18 U.S.C. § 1030)*
- *Customer Proprietary Network Information (47 U.S.C. § 222)*
- *Driver's Privacy Protection Ac (18 U.S.C. § 2721)*
- *Drug and Alcoholism Abuse Confidentiality Statutes (21 U.S.C. § 1175; 42 U.S.C. § 290dd-3)*
- *Electronic Communications Privacy Act (18 U.S.C. § 2701, et seq.), aka Stored Communications Act*
- *Electronic Funds Transfer Act (15 U.S.C. § 1693, 1693m)*
- *Employee Polygraph Protection Act (29 U.S.C. § 2001, et seq.)*
- *Employee Retirement Income Security Act (29 U.S.C. § 1025)*
- *Equal Credit Opportunity Act (15 U.S.C. § 1691, et. seq.)*
- *Equal Employment Opportunity Act (42 U.S.C. § 2000e, et seq.)*
- *Fair Credit Billing Act (15 U.S.C. § 1666)*

List of U.S. Laws Impacting Data Privacy and Security (cont.)

- *Fair and Accurate Credit Transactions Act of 2003*
- *Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.)*
- *Fair Debt Collection Practices Act (15 U.S.C. § 1692, et seq.)*
- *Fair Housing Statute (42 U.S.C. § § 3604, 3605)*
- *Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)*
- *Freedom of Information Act (5 U.S.C. § 552) (FOIA)*
- *Genetic Information Nondiscrimination Act (P.L. 110-233, 122 Stat. 881)*
- *Gramm-Leach-Bliley Act (15 U.S.C. § § 6801, et seq.)*
- *Health Insurance Portability and Accountability Act (Pub. Law No. 104-191 § §262,264: 45 C.F.R. § §160-164))*
- *Health Research Data Statute (42 U.S.C. § 242m)*
- *HITECH Act (Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5)*
- *Mail Privacy Statute (39 U.S.C. § 3623)*
- *Paperwork Reduction Act of 1980 (44 U.S.C. §3501, et seq.)*
- *Privacy Act of 1974 (5 U.S.C. § 552a)*
- *Privacy Protection Act (42 U.S.C. § 2000aa)*
- *Right to Financial Privacy Act (12 U.S.C. § 3401, et seq.)*
- *Tax Reform Act (26 U.S.C. § §6103, 6108, 7609)*
- *Telecommunications Act of 1996 (47 U.S.C. § 222)*
- *Telephone Consumer Protection Act of 1991 (47 U.S.C. § 227)*
- *U.S.A. Patriot Act (Pub. L. 107-56) (bill extending three anti-terrorism authorities signed 02/25/11)*
- *Video Privacy Protection Act of 1998 (18 U.S.C. § 2710)*
- *Wiretap Statutes (18 U.S.C. §2510, et seq.; 47 U.S.C. § 605)*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Basic Template for Federal and State Privacy Laws

- *Define the type of "non-public personal information" ("NPI") that is being regulated*
- *Provide that NPI must be protected from disclosure to unauthorized holders unless "anonymized" or "aggregated"*
- *Requires the development, implementation, maintenance and monitoring of comprehensive, written information security programs:*
  - *Collect only needed information*
  - *Retain only as long as necessary*
  - *Provide access only to those with a legitimate business purpose*
  - *Implement specific administrative, physical and electronic security measures to ensure protection*
- *Require prompt notice to individuals whose NPI is compromised*
- *Provides for the imposition of penalties for breaches by NPI custodians*
- *Requires the disposal of personal information in such a way that it cannot be read or reconstructed after disposal*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Practice Issues: What Should You Be Doing About This?

Risk Assessment:

- *What is it, who should conduct it and how should it be conducted?*
- *Perform a risk assessment/gap analysis*

Policy Development: Adopt a comprehensive Personal Information Security Policy, addressing policies are needed and the role of in-house and outside counsel in their development.

Education and Training:

- *Form an Information Security Committee to help implement the new policy*
- *Determine who should train corporate personnel and what role in-house counsel plays in that process*

Breach Detection and Response:

What is in-house counsel's role in responding to a breach?

- *Notice:*
  - *To federal/state agencies;*
  - *To those impacted by the breach as both a matter of state law and risk management*
- *Mitigation*

The role of notice and credit monitoring

In post-breach public statements, what key points should be included to minimize litigation risk?

To what extent can a company be liable for lost data?

How much can a typical breach cost a company both in time, brand equity and internal distraction?

What kind of insurance, if any, can a company use to offset costs?

- *Does it really help cover the costs?*

The role of outside counsel

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Preparing for a Breach

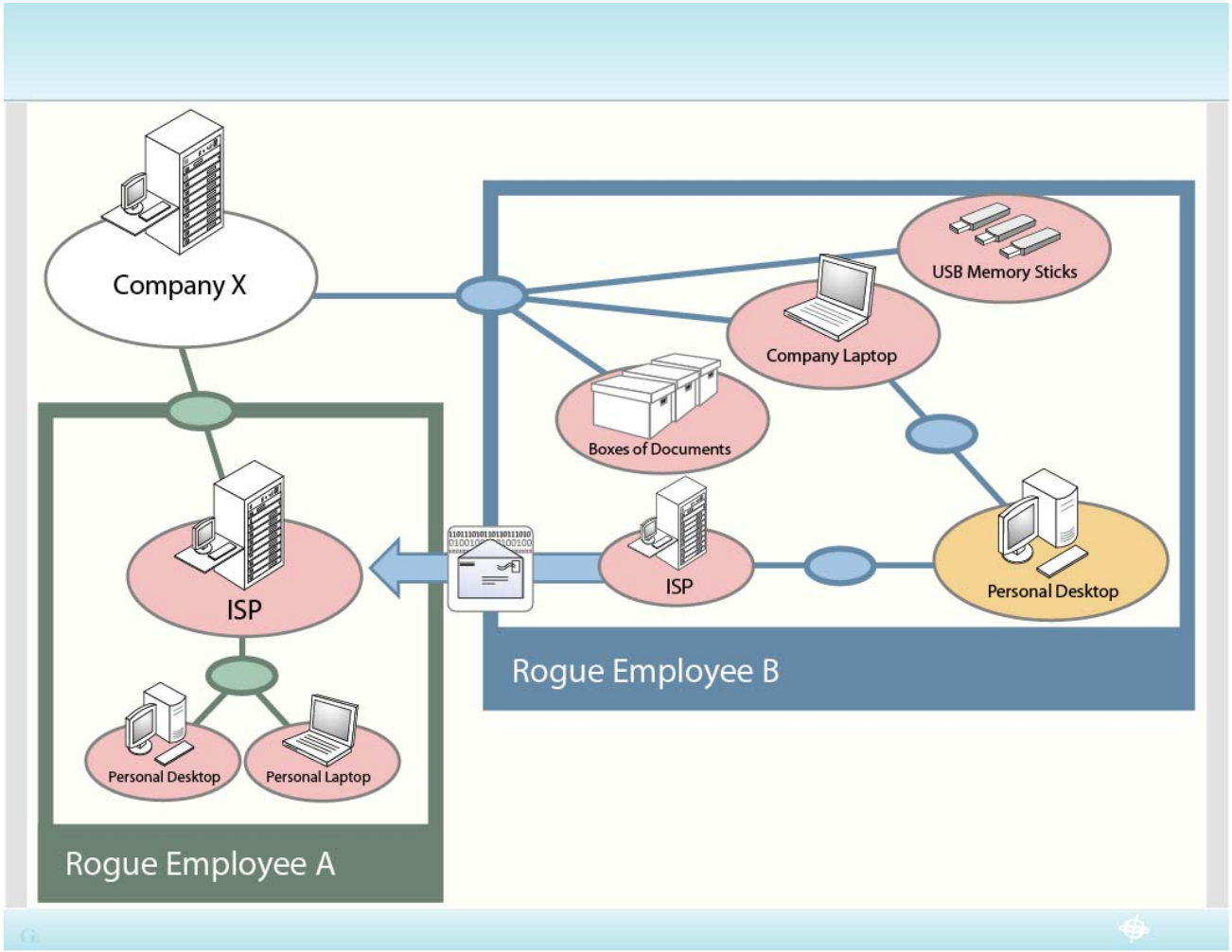
- *Incident investigation and response*
- *Breach notification and resolution*
- *Anticipate government investigations and possible litigation, as well as consumer litigation*
- *Press/public relations strategy*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Common Data Breach Scenarios

- *Accidental Breaches*
- *Faithless Employee/Ex-Employee*
- *Hackers & Thieves / Organized Crime*
- *Competitive Espionage*

Anatomy of a Data Breach



Legal Framework in a Data Breach

Customer Privacy Laws

- *Federal and state identity theft laws and regulations*
  - *Requiring customer notice*
  - *Requiring information security programs*
- *HIPAA / Medical information regulation*
- *Gramm Leach Bliley / Financial information regulation*
- *Regulations for specific industries (e.g., FCC CPNI Regulations)*
- *Laws governing specific information (e.g., Social Security number statutes)*
- *Negligence / Consumer protection laws*

Authorized Use Statutes

- *Computer Fraud & Abuse Act (CFAA)*
- *Electronic Communications Privacy Act (ECPA)*
- *Stored Communications Act (SCA)*

Surveillance / Information Security Law

- *Federal & State Wiretapping Statutes*
- *Invasion of Privacy*

Property Law

- *Larceny / Conversion*
- *Trade Secrets*
- *Copyright / Digital Millennium Copyright Act (DMCA)*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Social Media and Consumer Marketing: the FTC Approach

- *Privacy by design:*
  - *Incorporate substantive privacy protection into corporate practices from the ground up, such as in data security, collection limits, retention practices and maintaining data accuracy*
  - *Maintain comprehensive data management procedures throughout life cycle of products and services*
- *Simplify choices for consumers*
- *Achieve transparency to users:*
  - *Shorter, clearer privacy notices*
  - *Reasonable consumer access to the data they maintain*
  - *Prominent disclosures and express consent before using data in a materially different manner than claimed when the data was collected*
  - *Educate consumers*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Social Media and Consumer Marketing: the Department of Commerce Approach

Fair Information Practice Principles (FIPPs)

- *Transparency: Organizations should be transparent and notify individuals regarding collection, use, dissemination and maintenance of personally identifiable information*

FIPPs would be supplemented by "voluntary enforceable industry codes":

- *Relevant multi-stakeholder process for proposing new codes*
- *Approved and enforced by FTC*
- *Compliance is a safe harbor*

FTC would enforce FIPPs

- *Unclear if there would be federal private rights of action or federal pre-emption*

Adhering to the E.U. Privacy Directive

- ***E.U. Directive 95/46/EC***
  - *Addresses the collection, use, processing, and free movement of personal data.*
  - *Broad definition of "personal data" – "any information relating to an identified or identifiable natural person."*
  - *Each E.U. member state is required to enact implementing legislation.*
  - *Raises concerns for European-based companies, U.S.-based companies, and for companies who provide services to companies who are subject to the Directive.*
  - *Impacts "data controllers," "data processors," and data transfers.*

E.U. Privacy Directive – Key Points

- ***Data controllers**:*
  - ***Data collected only for "specified, explicit and legitimate" purposes. May not be in excess of what is needed for such purposes.***
  - ***Data must be accurate and up to date.***
  - ***Data must not be kept in a form that permits identification of the data subjects for any longer than is necessary.***

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

E.U. Privacy Directive – Key Points (cont.)

- ***Data Processors**:*
  - ***Data subject much give unambiguous consent to the processing; or***
  - ***Data processing must be necessary:***
    - *To the performance of a contract with the data subject;*
    - *To the performance of a contract to comply with legal obligations of the data controller;*
    - *To protect vital interests of the data subject;*
    - *For public interest reasons or the exercise of some official authority; or*
    - *For the purposes of legitimate interests pursued by the data controller or by third-party recipients of the personal data, provided such interests are not outweighed by the data subject's interests.*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

E.U. Privacy Directive – Key Points (cont.)

- ***Data Processors**:*
  - ***Data subject much give unambiguous consent to the processing; or***
  - ***Data processing must be necessary:***
    - *To the performance of a contract with the data subject;*
    - *To the performance of a contract to comply with legal obligations of the data controller;*
    - *To protect vital interests of the data subject;*
    - *For public interest reasons or the exercise of some official authority; or*
    - *For the purposes of legitimate interests pursued by the data controller or by third-party recipients of the personal data, provided such interests are not outweighed by the data subject's interests.*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

E.U. Privacy Directive – Key Points (con't)

- ***Data subjects have certain rights of access to personal data.***
- ***Heightened concern about "special categories" data (data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life)***
- ***European Commission has undertaken a review of the E.U. data privacy rules. Proposals expected in 2011.***

E.U. Privacy Directive – Data Transfers

Transfers permissible if to country that the European Commission has determined "ensures an adequate level of protection." United States does not qualify.

Other means:

1) ***U.S. Department of Commerce/European Commission: Safe Harbor Framework allows for data transfers to certified organizations.***
   - *Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission may participate in the Safe Harbor Scheme and may self-certify directly on the Department of Commerce's website.*
   - *Organizations that decide to participate in the Safe Harbor framework must comply with the Safe Harbor's requirements and publicly declare that they do so.*
2) ***Standard contractual clauses to safeguard data transfers.***
3) ***Article 26 Derogations (i.e., data subject has given his consent unambiguously to the proposed transfer).***
4) ***Intra-corporate transfers when multinational has adopted Binding Corporate Rules ("BCRs")***

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

U.S./E.U. - Safe Harbor Framework

- ***Safe Harbor requires organizations to comply with seven data privacy principles:***
  1) ***Notice***
  2) ***Choice***
     - ***Opt-in for sensitive information that may be disclosed to third party, or that may be used in manner other than for purpose for which it was originally collected.***
  3) ***Onward transfer***
  4) ***Access***
  5) ***Security***
  6) ***Data integrity***
  7) ***Enforcement***

The Federal Government Is Increasingly Focused on These Issues

- *In its 2012 Pentagon budget request, the Obama administration designated $2.3 billion to strengthen Department of Defense cyber security operations, including activities of the Pentagon's new Cyber Command and half a billion dollars for new cyber technology research. These figures do not include the growing spending on "black" cyber security activities, embedded within the approximately $80 billion annual intelligence budget.*
- *The Departments of Commerce, Defense, Homeland Security, Justice, and State are all actively developing cyber security initiatives. Earlier this year:*
  - *Secretary Clinton appointed Christopher Painter to head the new Office of the Coordinator for Cyber Issues, which will coordinate cyber security and other cyber issues across the Department and with other agencies.*
  - *Senator Lieberman reintroduced a comprehensive cyber security bill designed to protect the security of critical U.S. networks and communications system.*
  - *The Pentagon's cyber bureaucracy alone will include more than 40,000 personnel under the supervision of Cyber Command.*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Congress is Focused on Cyber- Security

"PRIORITIES FOR THE 112TH CONGRESS," from the GOP Technology Working Group:

"***Protect the U.S. from Cyber Attacks"***

"Cyber attacks have the potential to bring down our nation's economy, expose our most sensitive information, and even seriously injure or kill American citizens. We will work to enact strong cyber-security protections this Congress that focus on increasing protections in an innovative manner that allows for dynamic solutions to this dynamic problem."

Things to look for in 2011 and 2012:

- *Increased federal regulation in array of "hot" areas:*
  - *Comprehensive federal breach notice legislation, to pre-empt the many state rules*
  - *Cyber-security moves to the forefront:*
    - *More malicious code directed at military and manufacturing targets*
    - *New cyber-criminal incursions focused on theft of intellectual property and other "industrial espionage"*
  - *SEC filings to require cyber-breach/cyber-risk disclosures: Chairman Mary Schapiro said she will "seriously consider" issuing additional guidance outlining when public companies should disclose cyber-security breaches.*
- *Battle within government to see who regulates this field*
- *Increased government focus on national security aspects of security and privacy*
- *Increased corporate focus on internal cyber security programs*
- *More security breaches*

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Questions?

Speaker Contact Information

Colin J. Zick, Esq.
Foley Hoag LLP
czick@foleyhoag.com

Edward Palmieri, Esq.
Privacy Counsel, Facebook
ep@fb.com

Lex Mundi
www.lexmundi.com

LEX MUNDI
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

Association of Corporate Counsel

Thank you for attending another presentation from
ACC's Desktop Learning Webcasts

Please be sure to complete the evaluation form for this program as your comments and ideas are helpful in planning future programs.

If you have questions about this or future webcasts, please contact ACC at webcast@**acc.com**

This and other ACC webcasts have been recorded and are available, for one year after the presentation date, as archived webcasts at **http://webcasts.acc.com.**