Introduction to Corporate Information Security Law

Andrea M. Matwyshyn
a-matwyshyn@law.northwestern.edu
Adjunct Professor of Law, Northwestern University
Affiliate, Manufacturing and Technology Policy Programme
University of Cambridge
SOURCES OF LEGAL PROTECTION FOR PROPRIETARY INFORMATION AND SOURCES OF AFFIRMATIVE LEGAL PRIVACY OBLIGATIONS

- Sources of protection: (1) contract law; (2) trade secret law; and (3) federal intellectual property and computer intrusion law
- Multiple possible sources of privacy and security obligations exist and are specific to the type of information implicated
Benefits of leveraging law and agreements to protect proprietary information

- Preserving competitive advantage
- Limiting possible liability arising out of security breaches and unintended releases of information
I. SOURCES OF LEGAL PROTECTION FOR PROPRIETARY INFORMATION

- Contract law
- State level trade secret law
- Federal (and state) intellectual property law and computer intrusion law
1. Contract

- Agreements set forth the terms of services, compensation and data exchange between parties

- Services agreements (development, hosting, consulting, maintenance agreements)

- Employment Agreements

- Confidentiality Agreements
Services agreements generally include terms which set forth:

- Relationship of the parties
- Product and services specifications, benchmarks, and termination events
- Confidentiality and noncompetition obligations
- Recourse for breach and survival of obligations
- Consideration
- Intellectual property representations and warranties and ownership
- Limitations on liability
- Data control and use
- Derivative works and corollary rights
- Assignment
Employment agreements (and severance/termination agreements) with key employees generally include terms addressing:

- Confidentiality
- Assignment of inventions/ work for hire
- Noncompeting/nonsolicitation
2. Trade secret law

- Each state has a trade secret law, but the language of statutes varies.

- In order to fall within most trade secret statutes’ scope, information must:
  - Be included by the statute in its definition of “protectable information”
  - Satisfy certain security conditions under which protection is extended: (1) sufficient secrecy to derive value; (2) sufficiently reasonable efforts at protection.
Consistent information protection policies must be in place throughout the entity

- Usually a prerequisite for obtaining trade secret protection
- Confidentiality agreements with all employees and contractors
- Physical security
3. Federal law

- Intellectual property law
  - Copyright
  - Patent

- Criminal computer intrusion law
Copyright

- Federal legal protection for any original work of authorship fixed in a tangible medium
- Inherent copyright in any tangible work
- Filing with Copyright Office of Library of Congress
- Length varies by type of author
Patents

- Federal legal protection for 17 years to new, nonobvious, useful inventions

- Must disclose details for examination to U.S. Patent and Trademark Office

- Can be lengthy process and can be costly to enforce patents, particularly if challenged by deeper pockets
Criminal computer intrusion law

- Digital Millennium Copyright Act
- Computer Fraud and Abuse Act
- Electronic Communications Privacy Act
- Wire Fraud Act
- Various state statutes
- In certain instances such as large scale denial of service attacks, it may make sense to enlist governmental agencies’ help
II. SOURCES OF LEGAL PRIVACY OBLIGATIONS TO PROTECT CONSUMER INFORMATION

- Legally imposed
- Self-imposed
- Industry imposed
1. Legally imposed - Statutes

- Sensitive data
  - Children’s data
  - Financial information and data
  - Health data
  - Foreign data

- Other U.S. personally identifiable data and nonpersonally identifiable data
2. Self-imposed - Contract

- Website privacy policies are binding contracts that survive even in bankruptcy

- Online and offline data collection, control and use policies must comport

- Violations of privacy policies potentially subject entities to Federal Trade Commission investigation and civil liability
3. Industry imposed - Negligence

- Reasonable standards of care are determined on an industry specific basis

- Violations of industry norms of due care may give rise to liability to consumers in negligence

- Inquiry: Does the level of care exercised in a particular circumstance fall below the level of care a reasonable person or entity would have exercised in the same circumstances
III. HOW TO MITIGATE RISK

- View contracts as a historical record
- Make your contracts specific
- Think ahead and about what can go wrong
- Institute good entity-wide data control and security practices
1. Use contracts as a historical record of relationships

- Not just “papering” a transaction but a description of the relationship
- Protection from liability
- Demonstration of due care in the event of suit
2. Make contracts specific

- Specify information control practices
  - Encryption
  - Physical security
  - Limitations on access of third parties

- Shift costs of liability
  - Direct and indirect losses
  - Attorneys fees and costs
3. Think ahead

- Plan for the worst case scenario (while hoping for the best)

- Know the interests of the parties and the nature of the relationship

- Sometimes interoperability leads to liability

- Consult with legal counsel proactively; planning ahead is cheaper than fixing legal problems later
4. Institute good entity-wide information control practices

- Include an information control policy in employee handbook
- Put confidentiality agreements in place with all employees on all levels and with all third parties having physical or network access to proprietary information
- Enforce information policies regularly
- Have a Chief Privacy Officer
Thank you

Andrea M. Matwyshyn
a-matwyshyn@law.northwestern.edu