Information Compliance Overload:

Dealing with a Growing Corporate Legal Nightmare

Thomas J. Smedinghoff
Wildman Harrold
Chicago

It's Becoming a Major Concern

Wildman Harrold
Attorneys and Counselors

- "Regulatory requirements are growing exponentially."
- "A crush of costly regulatory demands has firms' compliance departments crying overload."
- "Firms are being required to dig out from under an unprecedented amount of new regulation."
- "We're under siege."
- "We're creating an environment where every [company] is out of compliance and violating rules at all times."
- "The overall cost to firms is immeasurable."

The Trend

Wildman Harrold
Attorneys and Counselors

- As businesses are going global …
- Information security regulation is increasingly becoming local

Information Security Obligations Come In Many Different Forms

Wildman Harrold
Attorneys and Counselors

- Laws
- Regulations
- Common law obligations
- System rules
  - (*e.g.*, ACH, federated identity, PKI)
- Contractual requirements
- Standards
  - (*e.g.*, PCI)
- And they often don't use the word "security"

Information Security Obligations Come From Many Different Jurisdictions

Wildman Harrold
Attorneys and Counselors

- State
- Federal
- International
- Associations / private systems
  - (*e.g.*, NACHA, SWIFT, credit card companies, etc.)
- Trading partners

Information Security Obligations Cover Many Different Issues

Wildman Harrold
Attorneys and Counselors

- Data privacy
- General data security
- Breach notification
- Credit card processing
  - PCI Standard
  - State PCI laws
- SSN
- RFID
- Spyware
- E-Discovery
- Record retention
- Record destruction
- E-mail retention
- Phishing
- Credit freezes
- Identity theft
- Financial information (SOX)
- Electronic delivery
- Electronic transactions
- Spam
- Consumer protection
- FCRA / FACTA
- Sector-specific regulations
- Pretexting
- Children
- Evidence

Information Security Obligations Come with Many Problems

Wildman Harrold
Attorneys and Counselors

- There are simply too many rules
  - On too many subjects
  - From too many different sources
  - How do you keep up?
- Many obligations are vague
  - E.g., What is “reasonable security”?
- Some obligations conflict with other obligations
  - E.g., SOX whistleblower vs. EU privacy
- Obligations may depend on status or data ownership
  - Controllers treated differently than processors
- Obligations added or change too rapidly

But Bad Things Will Happen If You Don't Comply

Wildman Harrold
Attorneys and Counselors

- Loss of benefits/protections/rights etc.
- Compliance liability (even w/o damage)
  - FTC and state AG enforcement actions
  - Regulator enforcement actions / penalties
  - EU Data Protection Authorities
- Liability to injured parties for damages
  - Government enforcement actions
  - Private causes of action
- Remediation costs
- Inability to enforce your rights (*e.g.*, AmEx case)
- PR risk
  - Injury to reputation - the ultimate penalty!

Some Thoughts on

Dealing With the Problem

Start With the Facts!

Wildman Harrold
Attorneys and Counselors

- Identify your data
- Identify your activities
- Assess your legal risks

Identify Your Data – Understand Your Information Attributes

Wildman Harrold
Attorneys and Counselors

- Identify your information
  - In your possession
  - In possession of third parties
- Understand your information attributes
  - Who owns it?
  - Who possesses it?
  - Who has access to it?
  - Where does it come from?
  - Where is it used / stored?
  - What is its sensitivity? Is it confidential?
  - How is it protected?

Identify Your Activities – Understand Your Information Lifecycle

Wildman Harrold
Attorneys and Counselors

- Collection / acquisition / creation of data
- Use of data in business
  - Internal purposes
  - Marketing
  - Other
- Electronic delivery / communication of data
- Transfer of data
  - To a new controller
  - For processing only
- Storage / retention of data
- Use of data in litigation
  - Production of data (e.g., discovery)
  - Use as evidence
- Destruction of data

Assess Your Legal Risks

Wildman Harrold
Attorneys and Counselors

- Like a security risk assessment
- What laws apply –
  - To your data?
  - To your use of that data?
- What is the likelihood of non-compliance?
- What is the penalty / liability for non-compliance?
- Prioritize

Involve All of the Stakeholders

Wildman Harrold
Attorneys and Counselors

- Coordination and information sharing is critical
- Need involvement of
  - Technical (IT) department
  - Relevant business functions
  - Legal
  - Board of Directors, C-Level executives, management,

Understand the Regulatory Structure -- The Lobachevsky Principle

Wildman Harrold
Attorneys and Counselors

- The method by which information security laws are developed was summarized about 40 years ago by the great (fictional) Russian mathematician Nicolai Ivanovich Lobachevsky, when he uttered those immortal words . . .

- "When you see an [*information security law*] you like, …
- "Don't shade your eyes . . .
- "Plagerize, plagerize, plagerize!
- "Only be sure please always to call it research."

Result – A Synergistic Process That Tends To Focus on the Same Issues

Wildman Harrold
Attorneys and Counselors

- Two trends –
  - Bi-directional sources of law
    - Some ideas that start local and are adopted globally
    - Other ideas start at international level, and are adopted locally
  - Interactive development of law unlike anything we've ever seen on a global scale
- Everyone is building on what everyone else has done
- Result – information security laws often follow the same structure and consider the same issues
- Result – common approaches, such as
  - Breach notification laws
  - SSN laws
  - Spam laws
- So focus on the issues first; then ask how each law addresses those issues

Focus on the Legal Trends

Wildman Harrold
Attorneys and Counselors

- Security
  - Expanding duty to protect corporate data
  - Definition of legal standard for “reasonable security”
  - Imposition of a duty to warn
- Privacy
  - Movement toward omnibus approach

Take a Holistic Approach

Wildman Harrold
Attorneys and Counselors

- Need a comprehensive scheme to manage all compliance obligations
- Don’t do it piecemeal within a category
  - E.g., don’t address SOX security but ignore PII security
- In other words, when dealing with a specific topic (e.g. security)
  - Don’t comply with some rules but not others
  - Don’t comply for some data, but not other data

Options re Possible Approaches

Wildman Harrold
Attorneys and Counselors

- "Bury you head in the sand" approach
  - "Close your eyes and hope for the best"
- The single jurisdiction approach
  - E.g., Canada-only, California-only, or U.S.-only, etc
- The 80-20 approach
  - Focus on major issues, or focus on where you do most business; prioritize
- Adopt most stringent requirements everywhere
- Comprehensive jurisdiction-by-jurisdiction compliance approach

Doing the Right Thing

Wildman Harrold
Attorneys and Counselors

- Compliance often is more an interpretive art than an empirical science
  - Often involves risk-based decisions
  - It's not black & white; yes or no
- Companies should at least be able to show that they have made a good faith effort to comply with the law
- Document your discussions and decisions
  - Explain your reasoning at the time
  - Be able to show the regulators, the courts, and the press, that you considered the issues with best of intentions
  - Compare *Guin v. Brazos* with *Bell v. Michigan Council*

You Need to Try!

Wildman Harrold
Attorneys and Counselors

"We know that security can't be perfect, so we don't expect perfection. But companies need to try, and if you do that you will be much better off."

Jessica Rich
Assistant Director of the Division for Privacy and Identity Protection,
Federal Trade Commission

Further Information

Wildman Harrold
Attorneys and Counselors

Thomas J. Smedinghoff

Wildman Harrold

225 West Wacker Drive

Chicago, Illinois 60606

(312) 201-2021

smedinghoff@wildman.com