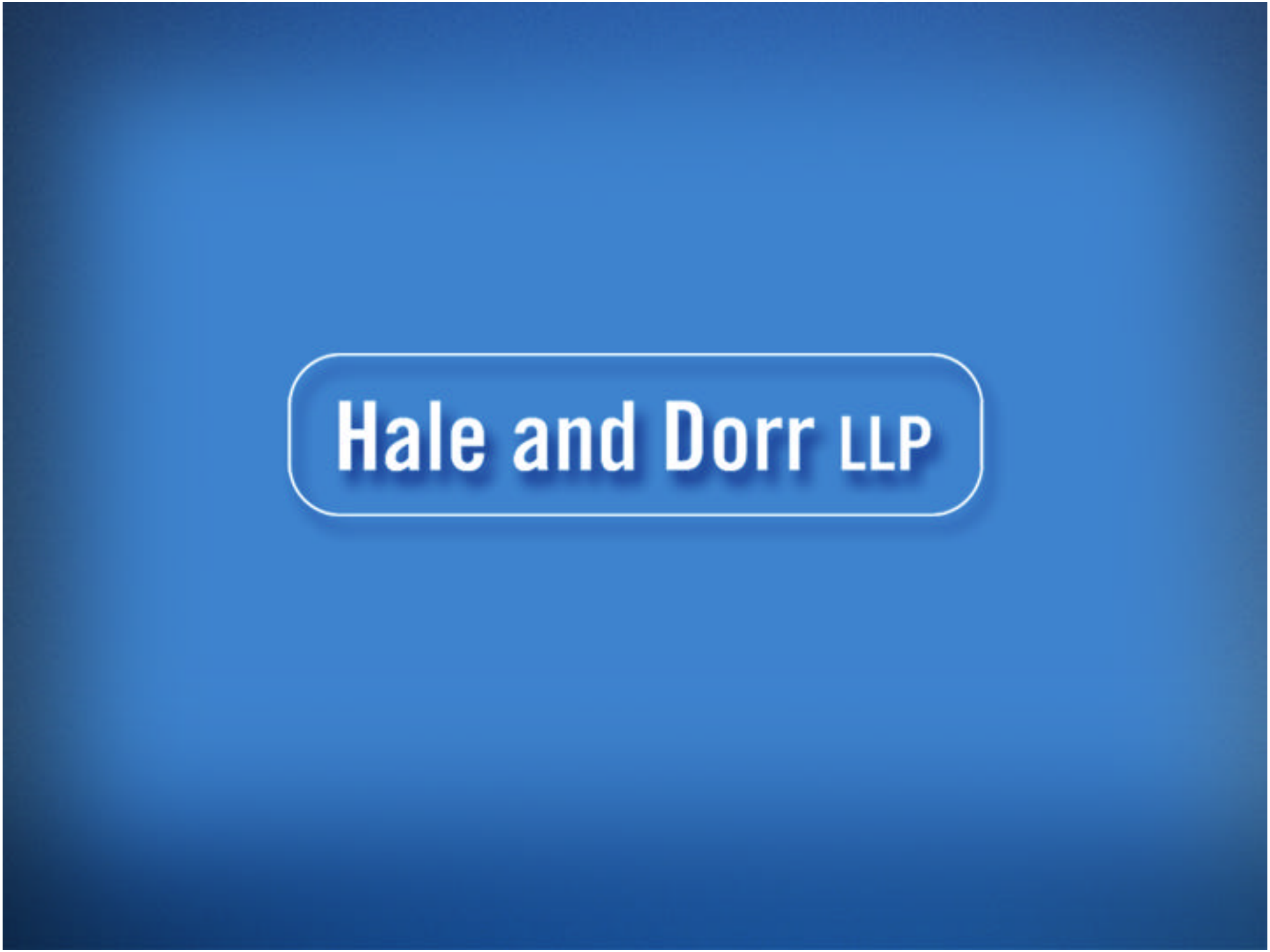

Hale and Dorr LLP

# Massachusetts Telecommunications Council
# Safe or Sorry? The Latest for the Security Front

## Legal Issues

Jorge Contreras

Hale and Dorr LLP

November 18, 2003

# Regulatory and Legal Landscape


- The security of data and personal information has come under increased scrutiny in recent years from a number of sources:
  - Federal Legislation
  - State Legislation
  - European Union
  - Government Enforcement
  - Common Law Liability

technology transactions + licensing

# Federal Legislation – HIPAA


- Health Insurance Portability and Accountability Act of 1996
- Privacy Rule
  - Must generally safeguard individually-identifiable health information
- Affected:
  - Covered Entities (health plans, healthcare clearinghouses, healthcare providers)
  - Business Associates (companies that perform or assist in use or disclosure of protected health information: claims admin, data processing, billing, actuarial, legal, etc.)

technology transactions + licensing

# Federal Legislation – HIPAA Security Rule


- Compliance Deadline – April 21, 2005 (2006 for small health plans)
- Must ensure confidentiality, integrity and availability
- Must protect against reasonably anticipated unauthorized uses and disclosures
- 18 Standards; 36 Implementation Specifications
  - Administrative measures
  - Physical security
  - Technical safeguards
  - Contractual requirements (with Business Associates)
  - Internal policies and procedures

technology transactions + licensing

# Federal Legislation - GLBA


- Gramm-Leach-Bliley Financial Services Modernization Act of 1999
- Requires agencies to establish regulations to
  - Ensure the security of customer financial data
  - Protect against anticipated threats to data security
- Traditional financial institutions (i.e., banks)
  - Board of Directors responsible for information security and development, implementation and oversight of written security program
    - Day-to-day handling may be delegated to management
  - Program must include access controls, encryption, monitors, response program
- FTC administration of non-traditional financial institutions
  - Includes mortgage brokers, financial advisors, appraisers
  - Must develop an appropriate information security program based on suggested guidelines

technology transactions + licensing

# State Legislation


- California Identity Theft Protection Act (SB 1386)
  - Became effective July 1, 2003
  - Any company that does business in the state must disclose data security breaches to those California residents whose unencrypted personal information was or reasonably might have been accessed
  - Company does not need to be located in California
  - Notice must be provided in the most expedient time possible and without unreasonable delay
  - Offers private right of action
  - Pending class action lawsuit against Microsoft
- Other states and federal govt. are considering similar identity theft bills that could impose additional reporting requirements

technology transactions + licensing

# European Union


- EU Data Privacy Directive
  - Data controllers must implement measures to protect personal data from accidental loss, alteration, unauthorized disclosure or access
  - Applies to all industries, unlike segmented regulations of U.S.
  - Personal data may not be transferred to U.S. or other countries that are deemed to have “inadequate” data protection laws
- Safe Harbor program
  - Allows U.S. companies to receive EU data
  - Must take reasonable precautions to protect EU data from loss, misuse, unauthorized access, disclosure, alteration and destruction

technology transactions + licensing

# Government Enforcement


- Eli Lilly (2002)
  - Employee mistake resulted in disclosure of email addresses of service subscribers
  - Action by FTC and state AGs
  - FTC Settlement Jan. 2002: steps required to ensure data security plus annual audit of security
  - State Settlement Jul. 2002: $160,000 fine plus strengthening of internal security measures, training and monitoring
- Ziff Davis Media Inc. (2002)
  - State attorney general actions (3 states)
  - Inadvertantly allowed personal information of 12,000 online magazine subscribers to be exposed to web surfers – including credit card information
  - Agreed to implement security measures and paid $100K fine and $500 payment to each person whose credit card information was exposed, even if not used

technology transactions + licensing

# Government Enforcement – 2


- Guess (FTC 2002)
  - Customer credit card data was available through web site to common hacker attacks (SQL injection)
  - FTC settled June 2003: required implementation of comprehensive info security program, must be certified
- ACLU (2003)
  - Individual data was accessible through ACLU website search in violation of ACLU privacy policy
  - NY AG action settled in Jan. 2003: required establishment and maintenance of data security program and compliance review
- Victoria's Secret (2003)
  - Website allowed browsers to view other customers' orders
  - NY AG action settled Oct. 2003: $50,000 fine

technology transactions + licensing

# Common Law Liability


- TriWest Healthcare Alliance (2002)
  - Computer hardware physically stolen containing health information of 562,000 military personnel, retirees and family
  - $1M in legal fees + $100,000 reward offer for information
  - Class action lawsuit filed claiming negligent security standards – dismissed Oct. 2003 due to lack of proven damages
- Possible Causes of Action
  - Regulatory noncompliance
  - Negligence (for failure to secure)
  - Breach of Contract (violation of privacy policy)
  - Product liability (for failure to be secure)

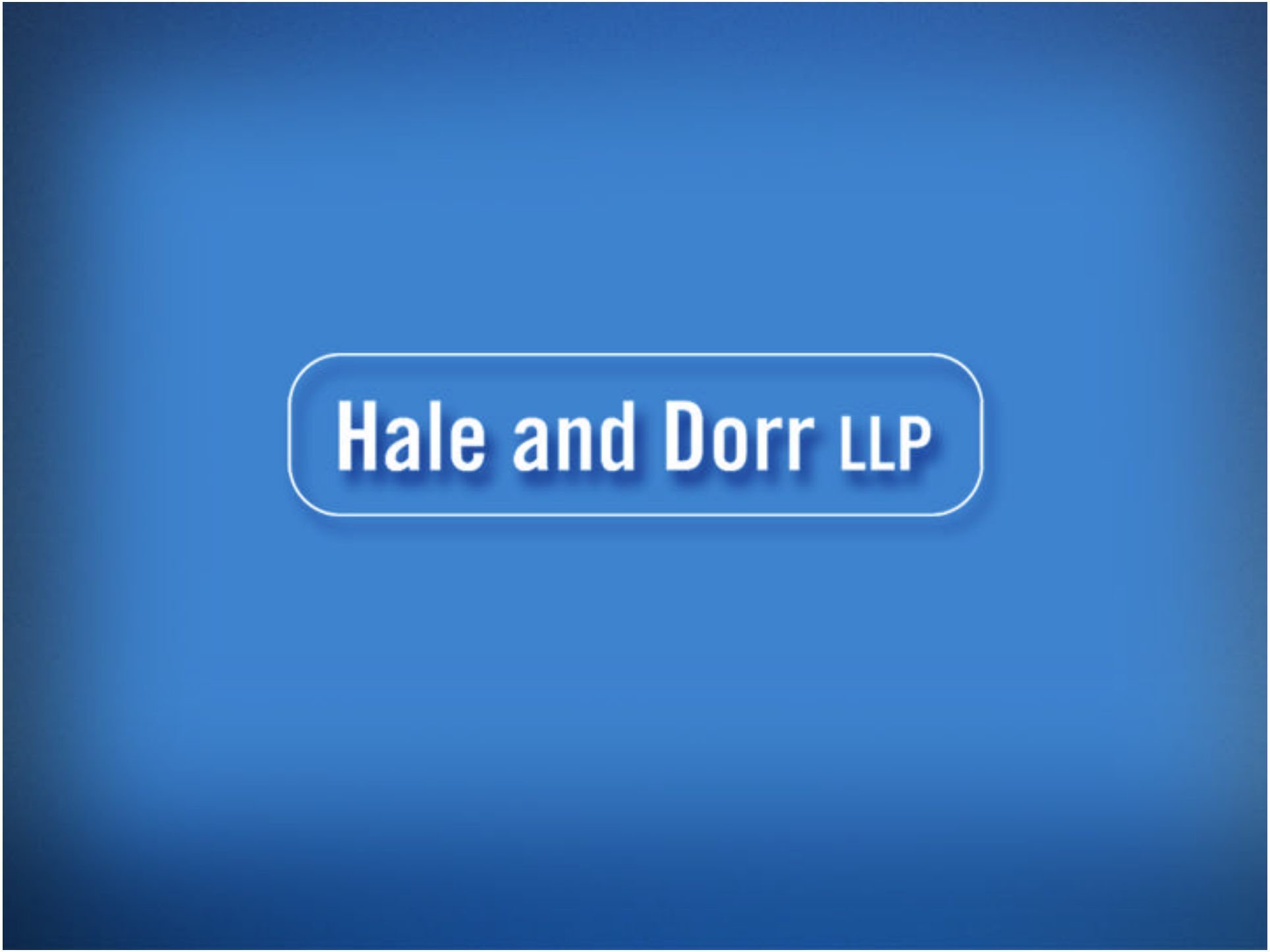
technology transactions + licensing

# For Further Information

Jorge Contreras
Hale and Dorr LLP
60 State Street
Boston, MA 02109
617-526-6872
jorge.contreras@haledorr.com

Jeff Munsie
Hale and Dorr LLP
60 State Street
Boston, MA 02109
617-526-6239
jeffrey.munsie@haledorr.com


technology transactions + licensing


Hale and Dorr LLP