Legal Ethics in the Information Age: Unique Data Privacy Issues Faced by Law Firms

v2.18.11, rev
Presenters

• Joseph DeMarco, Partner
  DeVore & DeMarco, LLP

• Lauren Shy, Assistant General Counsel
  Fragomen, Del Rey, Bernsen & Loewy, LLP

• Aaron Simpson, Partner
  Hunton & Williams, LLP

Note: The presenters do not practice in the fields of legal ethics or professional responsibility. The information provided in this presentation is not intended to be legal advice and should not be interpreted as such. The experiences, views and opinions expressed are those of the presenters and not necessarily those of their employers or the IAPP.
Overview

I. Ethical Obligations
   – Law firm data collection
   – Review of select ABA Rules, ethics opinions

II. Legal Issues
   – Moving beyond ethical obligations
   – Recent decisions impacting law firms
   – Daily encounters with data privacy laws

III. A Practical “Framework”
Law Firms are Not Immune

- Privacy issues have become ubiquitous for all businesses
- Law firms are no exception, in fact they face unique challenges
  - Must comply with evolving privacy requirements
  - Varying client requests
  - But also must comply with ethical obligations
Personal Data Collection by Firms

• Personally identifiable information (PII) is routinely collected
• Necessary to provide legal services in some matters
  – e.g., Employment, Trust & Estates, Immigration, Information Security
  – Can be sensitive in nature
    • Religion, national origin, political affiliation, criminal background, SSNs, financial account information, medical history
Data Processing

• Data may be disclosed by the firm to
  – Colleagues in other jurisdictions
    • For business or HR purposes
  – Third party service providers
    • Payroll
    • Benefits
    • Data hosting facilities
    • Technical support
    • Records management
Storage of Personal Information

• Storage of both hard-copy and electronic records creates risk
  – Mobile devices particularly risky
  – Breaches involving stolen laptop computers with unencrypted hard drives particularly costly
  – Storage of data in the cloud has become commonplace
    • Provides the ability to leverage economies of scale, geographic distribution, and automated systems to drive down costs
    • BUT, must consider the privacy and information security issues
  – Inadvertent storage of personal information on printers and fax machines
Data Retention & Destruction

• Data retention
  – How long must you keep personal information in the client files context?
    • ABA - Materials On Client File Retention
      [link to ABA guidelines]
    • N.Y. State Bar Ass’n Comm. On Prof’l Ethics, Op. 460, 1977 WL 15688 (1977); N.Y. City Bar Association, Formal Opinion 2010-1: Use of Client Engagement Letters To Authorize the Return or Destruction of Client Files at the Conclusion of a Matter
    • Restatement (Third) of Law: The Law Governing Lawyers
  – What is client “property”
    • Majority view

• Secure destruction of personal information
  – Legal requirement at both state and federal level
    • Cross-cut Shredding, degaussing
    • State bar opinions (Oregon State Bar Formal Ethics Op 2005-141(law firm may contract with recycling service to dispose of documents that may contain information relating to the representation of a client.)
Ethical Obligations

• ABA Model Rules of Professional Conduct
  – Rule 1.1 – Competent Representation
  – Rule 1.6 – Confidentiality
  – Rule 1.9(c) – Former Client
  – Rule 1.15 – Client Property
  – Rule 1.18 – Prospective Client
  – Rule 5.3 – Supervising non-lawyers

• Your state rules may differ . . . .
Ethics Opinions – Samples*

- In addition to the recent FL opinion, see:
  - **Arizona 08-02**: Client Files; Confidentiality of Information; Safekeeping Property; Duty as to Client Property – “The (retention) policy should be closely tailored to meet the client’s needs, taking into account, applicable statutes of limitations, substantive law, and particular circumstances likely to arise from the nature of the representation.”
  - **Arizona 05-04**: Electronic Storage & Confidentiality - “Competent and reasonable steps . . .”
  - **California 2010-179**: The State Bar of California Standing Committee on Professional Responsibility and Conduct Formal Opinion - “Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use.”
  - **Maine 194 (2008)**- “We conclude that, with appropriate safeguards, an attorney may utilize transcription and computer server backup services remote from both the lawyer's physical office and the lawyer's direct control or supervision without violating the attorney's ethical obligation to maintain client confidentiality.”
  - **New York – NYSBA Eth. Op. 842 (2010)** - “Lawyer may use online data storage provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer’s obligations under Rule 1.6. Additionally, the lawyer should stay abreast of technological advances to ensure that storage remains sufficient to protect the client’s data and should monitor the laws of privilege to ensure that the online storage will not cause loss or waive privilege.”
Decisions

• In the litigation context, see *Stengart* decision in New Jersey
  – Employment dispute
  – Employer’s law firm read emails sent on employee’s webmail account using company computer
    • Emails were sent to her lawyer
    • Court held firm should have set aside privileged communications
    • Intersection of lawful employee monitoring and ethics rules
Ethics rules are the FLOOR . . .

- They are minimum requirements for lawyers and law firms.
- Evolving definition of “reasonable” . . .
- Check the rules/opinions in your state
- ABA Ethics 20/20: [http://www.americanbar.org/content/dam/aba/migrated/ethics2020/pdfs/clientconfidentiality_issuespaper.pdf](http://www.americanbar.org/content/dam/aba/migrated/ethics2020/pdfs/clientconfidentiality_issuespaper.pdf)
Legal Issues

- I thought privacy and information security laws don’t apply to us!
- Yes, there are *some* recent and noteworthy exemptions:
  - GLBA
    - But the Safeguards Rule has essentially become the norm anyways
    - Must develop, implement and maintain a written information security program to safeguard personal information
  - Red Flags Rule
- But these are the exception to the rule
Domestic and International

• Most laws apply to law firms just as they would to other types of businesses
  – International data protection requirements
    • Cross-border data transfer restrictions
  – Patchwork U.S. requirements
    • Hundreds of state and federal privacy laws
    • Section 5 of the FTC Act
    • Security breach notification requirements
Security Breach Notification

- 49 U.S. jurisdictions have security breach notification laws
  - California SB 1386 started the trend
- Now there’s a federal law (HITECH)
- The term “security breach” defines a broad range of activities
- Generally, the duty to notify arises when unencrypted computerized “personal information” was acquired or accessed by an unauthorized person
- “Personal information” is an individual’s name, combined with:
  - SSN
  - driver’s license or state ID card number
  - account, credit or debit card number, along with password or access code
- Legal requirements differ
- Must also consider international requirements and best practices
- Law firm data breaches
Service Provider Management

• If third parties will access personal information on the firm’s behalf, there is risk
• Request that existing key vendors provide information about privacy and information security policies and practices
• Mitigate risk through:
  – Due diligence
  – Protective privacy and information security contract language
    • Maintain PII in strict confidence
    • Use PII only for your company’s benefit
    • Comply with all applicable laws, industry standards and the company privacy policy
    • Develop, implement and maintain reasonable security procedures to protect PII from unauthorized access, destruction, use, modification and disclosure
  – Ongoing monitoring
Cross-Border Data Transfers

– Need a legal basis to transfer personal data outside of the EU
– If most transfers are coming back to the U.S., Safe Harbor is an option appropriate
  • Depending on your firm’s specialties, Safe Harbor certification could be a business differentiator
– Also can consider
  • Binding corporate rules
  • Model contracts
  • Consent
    – Can be an administrative challenge
    – Primarily effective only with respect to customers, not employees
Other Hot-Button Privacy Issues

• Employee privacy
  – Background checks: Use of social networking sites
  – Monitoring

• Prescriptive state information security laws
  – Massachusetts and Nevada, as applicable
  – In Massachusetts, firms must develop, implement and maintain a comprehensive written information security program to protect personal information, including:
    • Developing information security policies
    • Requiring service providers by contract to implement security measures for personal information
    • Implementing numerous computer system security requirements
  – State laws regarding collection and use of SSNs
The Risks

• From a legal perspective, the risks are substantial
  – FTC enforcement authority: Section 5 of the FTC Act
  – Most FTC privacy enforcement actions result from security breaches
    • Dave & Buster’s, Card Systems, Petco, ChoicePoint, Tower Records, DSW, Barnes & Noble.com, BJ’s Wholesale Club, Guess.com, Inc.
  – Division of Privacy and Identity Protection at the FTC
  – Contractual liability
  – Civil and criminal penalties or fines (particularly in the EU)
  – Reputational harm

• Ethics violations
  – Could include reprimand, suspension, disbarment
Yikes... What do we do?

- Breathe
  - Ongoing commitment
  - Changing laws and regulations
  - Variations among jurisdictions/industries
  - High level of sensitivity

- Establish a framework to address these laws, risks and concerns
Practical Framework

• Start by mitigating highest and most immediate risks
  – Inventory personal data maintained by the firm
  – Conduct risk assessment considering at least:
    • Employee training and management
    • Information systems design and information processing, storage, transmission and disposal
    • Responding to and preventing attacks, intrusions and systems failures
  – Fix vulnerabilities identified through the risk assessment
  – Oversee vendors
  – Continually evaluate and adjust information security program

• Set appropriate expectations internally
• Select outside counsel, as appropriate
  • “A lawyer who represents himself has a fool for a client”
Framework, contd.

• Develop foundation
  – Governance structure
    • Identify a point person with support from firm management
    • Consider a committee to manage the issues
  – Develop Centralized Oversight of Privacy Function
  – Information Security Incident Breach Procedure
  – Privacy and Information Security Policies
  – Human Resources Privacy Issues
Framework, contd.

- Train new hires and all staff regularly
  - Confirm attendance
  - Discipline for failure to participate
- Require NDAs and contracts for staff and appropriate vendors
  - Monitor compliance and take action against those who violate firm policies
Framework, contd.

– Cyberinsurance or Network Liability Insurance
– Review malpractice insurance coverage
– Stay abreast of changes in laws
  • Join list serves, bar committees and sections, and associations, for example:
    – ABA Section on Science & Technology Law
    – IAPP
    – BNA – Privacy Law Watch; Privacy & Security Law Report
    – Hunton Privacy Blog
  • Communicate with IT group, data hosting providers, outside counsel
Other Resources – General


• IAPP’s “Information Privacy” handbook, available at http://www.iapp.org
Other Resources – Law Firms


- “Protecting and Securing Confidential Client Data,” by Anthony Davis and Michael P. Downey at http://www.law.com/jsp/lawtechnologynews/PubArticle_LTN.jsp?id=1202474447879&slreturn=1&hbxlogin=1
Questions?

Joseph DeMarco: 212.922.9499, jvd@devoredemarco.com

Lauren Shy: 212.230.2861, lshy@fragomen.com

Aaron Simpson: 212.309.1126, asimpson@hunton.com
Thank you