Data Privacy, Data Security in the Digital Age

December 9, 2013

Corby Anderson

“You already have zero privacy. Get over it.”

– Scott McNealy, CEO, Sun Microsystems, Inc.

Why Is Privacy Important?

• Data is a corporate asset, like any other
• Corporate data is at a higher risk of theft or misuse than ever before
• Companies have obligations to protect data
  – Laws, regulations, guidelines
  – Contracts with third parties
  – Privacy policies for users of websites, other online features
Information Privacy, Security

- A matter of corporate governance:
  - Does your board review and approve top-level policies on privacy and IT security risks?
    - 23% - regularly
    - 28% - occasionally
    - 42% - rarely or never
  - Does your board review and approve annual budgets for privacy and IT security programs?
    - 28% - regularly
    - 10% - occasionally
    - 54% - rarely or never

Carnegie Mellon CyLab 2012 Report

Information Privacy, Security

- Data privacy, data security risks are not limited to financial, healthcare, utility sectors. Retail sector is vulnerable as well
  - Zaxby's reported finding malware at 100 of its 560 locations in 10 states that could extract names, credit and debit card numbers
  - Papa John's agreed to pay $16.5 million to settle a class action over claims that it sent unauthorized texts to customers in violation of the Telephone Consumer Protection Act

What’s the Potential Harm?

- Breaches of data privacy, data security can result in
  - Damage to reputation
  - Disruption of operations
  - Legal liability under new and amended laws, regulations, and guidelines, as well as under contracts
  - Financial costs
Types of Information

- Personally identifiable information (PII)
  - Can be linked to a specific individual (name, email or full postal address, date of birth, Social Security number, driver’s license number, account numbers
- Non-personally identifiable information (non-PII)
  - Anonymous or aggregate data (zip code, area code, city and state, gender, age
- Hybrid of PII and non-PII
  - Non-PII that, when linked with other data, can effectively identify a person (“persistent identifiers”)

Laws that Protect PI

- Data privacy laws govern businesses’ collection, use, and sharing of information about individuals
- Federal, state, and foreign laws apply
- Laws govern both physical and electronic security of information

U.S. Laws Are a “Patchwork”

- U.S. laws are a patchwork, developed by sector (compared to European Community’s uniform, centralized law)
- Challenges in determining
  - Which laws apply to which activities
  - How to comply when multiple, sometimes inconsistent, laws apply.
FTC Act

- Prohibits "unfair or deceptive practices in or affecting commerce." No need to prove intent.
- A practice is "unfair" if:
  - It causes or is likely to cause substantial injury to consumers
  - It cannot reasonably be avoided by consumers
  - It is not outweighed by countervailing benefits to consumers or to competition
- A representation, omission, or practice is "deceptive" if:
  - It misleads, or is likely to mislead, consumers
  - Consumers' interpretation of it is reasonable under circumstances
  - It is material

FTC Act

- Practices attacked by FTC as "deceptive":
  - Violating published privacy policies
  - Downloading spyware, adware onto unsuspecting users' computers
  - Failing to verify identity of persons to whom confidential consumer information was disclosed
- Practices attacked by FTC as "unfair":
  - Failing to implement reasonable safeguards to protect privacy of consumer information

SEC Disclosure Guidance

- Public companies must report "material" events to shareholders
- Events a reasonable investor would consider important to an investment decision
- Guidance clarifies:
  - "Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."
  - Disclosure of risk factors should be tailored, not generic
  - "We expect registrants to evaluate their cyber security risks."
Children’s Online Privacy Protection Act

• Applies to operators of commercial websites and online services that collect information from children under age 13
  – “No one knows you’re a dog on the internet.”
• Requires reasonable efforts to get verifiable consent of parent or guardian or to notify parent or guardian
• Requires notice of
  – What information is collected from children
  – How information is used
  – How information is shared

Children’s Online Privacy Protection Act

• Prohibits conditioning child’s participation in an activity on disclosure of more PI than is necessary
• Amendments effective July 1, 2013
  – Include geo-location information, photos, and videos in types of PI that cannot be collected without parental notice and consent
  – Provide streamlined approval process for new ways to get parental consent
  – Require website operators to take reasonable steps to release children’s PI only to companies capable of keeping it secure

CAN-SPAM Act

• Controlling the Assault of Non-Solicited Pornography and Marketing
• Prohibits fraudulent, abusive, deceptive commercial email
• “One-bite” rule:
  – Business may send unsolicited commercial email message, properly labeled, to consumer, with easy means for consumer to opt out. If the consumer opts out, business may no longer send emails
### CAN-SPAM Act

- Commercial email broadly defined as having primary purpose to advertise or promote commercial product or service
- Does not apply to transactional emails, which facilitate or give update on agreed-upon transaction
- Business must monitor third party handling email marketing to ensure compliance
- Pre-empts state statutes, but states may enforce sections of Act addressing fraudulent or deceptive acts, computer crimes, other advertising restrictions

### Telephone Consumer Protection Act

- Established national “Do Not Call” registry
- Regulates use of “automated telephone equipment” such as auto-dialers, artificial or pre-recorded voice messages, fax machines
- Prohibits transmission of a “call” using an “automatic telephone dialing system” without prior consent of called party
- Per FCC, “call” covers both voice calls and text messages (even texts for which called party is not charged)

### Telephone Consumer Protection Act

- Enforcement by federal or state authorities
- Individuals may bring civil actions
  - Papa John’s class action over text messages claimed violations of TCPA, Washington Consumer Protection Act
- Relief can include injunction, actual damages, statutory damages of $500 per violation, treble damages
Class Actions Over Privacy

- Raft of litigation since 2010
- Redressing data breaches
- Asserting rights under federal, state consumer privacy statutes
- Brought against companies that advertise on Internet, social networks, mobile app providers
- Litigation often follows investigations, enforcement actions by FTC, state Attorneys General

Best Practices

- Create “culture of security” from top down
- Make information security a risk management issue, as well as a technology issue
- Understand which laws apply, ensure compliance with them
- Think like a lawyer; ask questions like a geek

Best Practices: Privacy Audit

- Review, assess policies and practices for data
  - Collection
  - Storage
  - Use
  - Disclosure
  - Protection
  - Destruction
- Identify exposure to data privacy, data security risks
- Consider, implement changes to minimize risks
- Develop, adopt best practices going forward
Best Practices: Privacy Audit

- Key benefit: Shows that data privacy and security are not just IT issues; instead, they touch on all parts of the company
  - Audit gathers information not only from IT/IS personnel, but also from personnel with responsibility for legal, marketing, development, sales, supply chain, human resources, international
- Helps ensure visibility, responsibility, accountability for privacy, security issues

Best Practices: Privacy Policy

- Most fertile ground for legal liability
- How do you get, use, and share information?
- Does what you say match what you do?
  - “We will never share your information . . . “
- Can people understand what you say?

Best Practices: Privacy Audit

- Review contracts with vendors that collect or provide PI to company
- Do contracts have indemnification provisions? Does vendor have resources to indemnify?
- Review potential insurance coverage
  - Property, liability (E&O, D&O, general liability, umbrella), computer crime, business owner package
Best Practices: Privacy Audit

- Consider class action waivers, arbitration provisions in terms of use, other consumer contracts
- Conduct annual reviews of
  - Data security
  - Data privacy
  - Risk management programs
- Develop contingency plans

Handling a Breach

“There are two kinds of companies: those that have been hacked and those that will be hacked.”

“There are two kinds of companies: those that have been hacked and know it and those that have been hacked but don’t know it.”

Handling a Breach

- If a security breach occurs
  - Do not panic
  - Do not overreact
  - Get facts: nature and scope of breach
  - Prevent further unauthorized access
  - Preserve evidence, work with law enforcement (your fren-emy?)
  - Notify vendors (such as payment processors)
  - Notify insurers
Handling a Breach

• If a security breach occurs
  • Determine whether customers must be notified
  • Review statutory requirements of all jurisdictions with residents whose PI has been compromised
  • Put yourself in shoes of person whose PI has been compromised
  • Apologize and accept responsibility
  • If notice is required, give it promptly
  • Offer a contact person
  • Do not forget to alert those “on the front lines”

Questions?

Corby Anderson
canderson@nexsenpruet.com
ext. 5331

Hot Topics in Workplace Privacy: Social Media and Smartphones

December 9, 2013
David Dubberly
Certified Employment and Labor Law Specialist
Workplace Privacy In The News

• Using social media postings to screen out applicants

Workplace Privacy In The News

• Discipline for critical social media posts

Workplace Privacy In The News

• New issue: accessing personal devices to monitor compliance with policies
Social Media and Background Checks

- **Main downsides**
  - TMI/discrimination claims
  - Some sites may be considered “consumer reporting agency” for purposes of FCRA
- **Best practices**
  - Not decision makers
  - Same protocol for all applicants
  - Only public info./no deception
  - 12 states have enacted password protection legislation
  - Only job-related info.

Social Media and Discrimination/Harassment

- **Title VII, ADEA, and ADA**
  - Prohibit discrimination, harassment, and retaliation
  - Employer liability for actions by supervisor
    - Liable if results in “tangible employment action,” but may avoid liability if exercised reasonable care to stop
  - Employer liability for actions by co-worker
    - May avoid liability if exercised reasonable care to stop

Social Media and Discrimination/Harassment

- **ADA**
  - “Medical records” treated as private and kept in separate confidential file
- **GINA**
  - Don’t use genetic info., including family medical history, in employment decisions
  - Don’t request, require, or purchase genetic info. about job applicants and employees
  - Inadvertent acquisition exception
**Deneau v. Orkin, LLC**  
(S.D. Ala. May 20, 2013)

- Employee on FB: “anyone know a good EEOC lawyer? need one now”
- Manager saw post and faxed to division HR manager
- One week later, employee terminated for repeatedly working overtime without authorization
- Employee sued for Title VII retaliation, etc.
- Court: FB post = protected activity, and based on temporal proximity employee established prima facie case
- But SJ for employer because no proof its legitimate, non-discriminatory reason was pretext

**Social Media and Labor Law Compliance**

- National Labor Relations Act Sec. 7
  - Employees have right to organize or join unions and to engage in other concerted activities for purpose of mutual aid and protection
  - Protects disparaging statements about company and employees
  - Protects discussion of compensation
  - Does not protect harassment

**Target Corp.**  
(NLRB Apr. 26, 2013)

- Info. security policy: employees prohibited from disclosing confidential info. relating to company or employees on social media, in break rooms, at home, or in open areas and public places
- Term “confidential info.” broadly defined as “non-public company info.” including “team member personnel records”
- ALJ: Policy violated employees’ Sec. 7 right to discuss wages, hours, and working conditions
  - Target ordered to cease and desist from maintaining overly broad policy
- NLRB: Upheld ALJ’s decision and order
Social Media and Trade Secret Protection

- S.C. Trade Secrets Act
  - Trade secret info. must be “the subject of efforts that are reasonable under the circumstances to maintain its secrecy”
  - Reasonable measures may include:
    - Confidentiality agreements
    - Policy prohibiting improper disclosure
    - Security software for mobile devices
    - Strong passwords
    - Immediate report of lost or stolen device
    - Exit interview procedures

Social Media and ECPA Compliance

- Computer wiretap laws
  - Electronic Communications Privacy Act as amended by Stored Communications Act
  - Criminal offense to access stored electronic communications “without authorization”
  - Also creates civil cause of action
  - State computer crimes laws similar


- Nurse posted comment on private FB account critical of paramedics for saving life of Holocaust Museum shooter
- Co-worker who was FB friend voluntarily showed screenshot of comment to supervisor
- Hospital fired nurse for post and accumulated disciplinary actions
- She sued under SCA and for common law invasion of privacy

- Hospital won summary judgment
- Court: FB post was stored electronic communication protected by SCA
- But since it was accessed by an authorized FB friend, Hospital did not violate statute by viewing it
- Also, Hospital did not invade employee’s privacy because it was “passive recipient” of info. it “did not seek out or ask for”

**Social Media and FTC Compliance**

- Federal Trade Commission
  - Social media posts can be advertising
  - Employer liability if employee promotes products or services on social media
    - Without disclosing employment status
    - Using false or misleading statements

**Smartphones in Workplace**

- Transition from company-issued BlackBerrys to employee-owned smartphones and tablets
  - Connect personal devices to employer e-mail and data networks
  - Create, store, and transmit work-related info on personal devices employer does not control
  - Trend referred to as “Bring Your Own Device”
Smartphones in Workplace

- 80% of smartphones used for work are employee owned (McKinsey survey June 2012)
- 30% of employers require employees to sign BYOD agreement (Ovum survey Nov. 2012)
- 50% of employees who left or lost jobs in last 12 months admitted taking confidential info. (Ponemon Institute survey Mar. 2013)

BYOD and CFAA Compliance

- Computer hacking laws
  - Computer Fraud and Abuse Act
    - Criminal offense to access computer “without authorization”
    - Permits recovery of money damages if such access results in damage of over $5,000
  - State computer crimes laws similar

BYOD and FLSA Compliance

- Fair Labor Standards Act
  - Exempt vs. non-exempt employees
  - Unpaid off-the-clock work
  - Unpaid overtime
BYOD and OSHA Compliance

• Occupational Safety and Health Act
  – Repetitive stress injuries
  – Distracted driving

---

**Sitton v. Print Direction, Inc.**
(Ga. Ct. App. 2011)

• Employee used personal laptop connected to employer’s network for work
• Also used it to send business to competing business started by his wife
• While employee away from office, CEO entered his office, moved computer’s mouse, clicked on e-mail listing in personal account that appeared on screen, and printed e-mails showing disloyal conduct
• Employee terminated, then sued under GA computer crimes statute and for common law invasion of privacy

---

**Sitton v. Print Direction, Inc.**
(Ga. Ct. App. 2011)

• Trial court ruled for employer and awarded $39,000 in damages
• Appeals court affirmed
  – CEO’s actions not prohibited by GA statute because they were not “without authority”
    • Employer’s policy on computer use, which allowed inspection of electronic devices in course of investigation, applied to personal equipment
  – CEO’s actions not unreasonable invasion of privacy under circumstances
Lazette v. Kulmatycki  
(N.D. Ohio June 5, 2013)
- Employer issued BB to employee
- She set up personal G-mail account with employer’s permission
- Employee left and turned in BB
- She thought she had deleted G-mail account, but she hadn’t
- Supervisor allegedly read 48,000 emails in G-mail account and shared some
- Employee sued supervisor and employer under SCA and for common law invasion of privacy

Lazette v. Kulmatycki  
(N.D. Ohio June 5, 2013)
- Court denied motions to dismiss
  - As to SCA claim and unopened e-mails: “The mere fact that [supervisor] used a company owned [BB] to access plaintiff’s e-mails does not mean that he acted with authorization when he did so.”
  - As to privacy claim: the e-mails were “highly personal and private” and “a reasonable jury could find [supervisor’s] reading of tens of thousands of such private communications, if proven to have occurred, highly offensive.”

BYOD Policy and Consent Form
- What to do if device lost or stolen
- What employer data can be downloaded to personal device
- Employer not liable for lost or damaged personal data
- Signed consent for employer to monitor, access, and remotely delete data in specified circumstances
- Signed consent for employer to install security software and applications to protect its data
WHAT EVERY BUSINESS NEEDS TO KNOW ABOUT HIPAA (YOU MAY BE SORRY IF YOU DON’T ASK)

December 9, 2013
Jeanne M. Born, RN, JD

What everyone knows about HIPAA and Privacy of health information

• Applies to medical/health care information created and maintained by health care providers.
• HIPAA protects the privacy and security of medical/health care information.
What everyone should know about HIPAA and Privacy of health information

• HIPAA has a broader brush than just healthcare

• Applies to Covered Entities (CEs)
  – Health care providers (that transmit PHI in a HIPAA covered transaction)
  – Health plans
  – Healthcare clearinghouses

• Applies to Business Associates of CEs

What everyone should know about HIPAA and Privacy of health information

• Health information is more than just medical information:
  – any information, including genetic information, whether oral or recorded in any form or medium, that
  – (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
  – (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

What everyone should know about HIPAA and Privacy of health information

• Individually identifiable health information (IIHI) is information that is a subset of health information, including demographic information collected from an individual, and:
  • Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
  • Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  • That identifies the individual; or
  • With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
What everyone should know about HIPAA and Privacy of health information

- Protected health information (PHI) means IIHI that is:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.

- PHI excludes IIHI:
  - In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
  - In records described at 20 U.S.C. 1232g(a)(4)(B)(v);
  - In employment records held by a covered entity in its role as employer; and
  - Regarding a person who has been deceased for more than 50 years.

What Companies DO KNOW:

- “OBAMACARE” - As of January 1, 2015, all employers of 50 or more full-time employees must provide access to health insurance or face monetary penalties.

What Companies May Not Know

- Companies providing health insurance for the first time.
- What the Company’s health plan HIPAA obligations entail:
  - Fully-insured and fully administered plans.
  - Self-insured plans that are either self-administered or administered by a third party administrator (TPA).
HIPAA Requirements: Fully Insured and Administered Plans

- Fully-insured and fully administered plans:
  - Amend plan documents to allow sharing of information if necessary.
  - Provide the Health Plan’s Notice of Privacy Practices (NPP) upon request.
  - Refrain from retaliatory or intimidating acts for making HIPAA complaints.

HIPAA Requirements: Self Insured and Either Self-Administered or Administered by TPA

- Enter into appropriate business associate agreements (BAA);
- Amend the plan documents to allow sharing of information;
- Institute procedures to comply with plan amendments;
- Use and disclose PHI only as allowed under the Privacy Standards;
- Have all policies and procedures required under the Privacy and Security Standards;
- Provide plan participants with the NPP.

Privacy Policies and Procedures

- Designate a privacy official
- Train your employees
- Safeguard the PHI
- Handle Complaints
- Sanction violations
- Refrain from retaliation for making complaints about your privacy practices
### Privacy Policies and Procedures

- Provide for participants’ rights:
  - Access
  - Amendment
  - Accounting
  - Restrict uses and disclosures
  - Confidential communication
  - Receive notice of the Company’s privacy practices
  - Receive notice of breaches of unsecured PHI

### Security Policies and Procedures

- Required security risk analysis
- Required development of security measures to decrease risks/vulnerabilities identified.
- Administrative safeguards
  - Security Officer
  - Sanctions
  - Workforce access policy to authorize access/create clearance procedures/create termination procedures
  - Information access policy
  - Security awareness/training program
  - Security incident procedures (response and reporting)
  - Contingency plans
    - Data backup plan
    - Emergency mode operation plan
    - Testing and revision procedures
    - Assess application/data criticality
  - Evaluation policy
  - Business Associate policy

### Security Policies and Procedures

- Physical Safeguards:
  - Facility Access Controls
    - Contingency operations
    - Facility security plan
    - Access control and validation
    - Maintenance records
  - Workstation Use Policies
  - Workstation Security Policies
  - Device and Media Control Policies
    - Disposal
    - Re-use
    - Accountability of hardware
    - Data backup and storage
Security Policies and Procedures

• Technical Safeguards
  – Technical Access Control
    • Unique user id
    • Emergency access procedure
    • Automatic logoff
    • Encryption/decryption
  – Audit controls (record hardware and software activity)
  – Integrity policies (protect from alteration & destruction)
  – Person/Entity authentication
  – Transmission Security
    • Integrity controls
    • Encryption

Privacy & Security Policies and Procedures

• Especially be sure that no health plan information is disclosed to or used by the employer to make employment decisions:
  – Potentially subject to enforcement penalties
  – Recent rule changes have greatly ratcheted up the penalty provisions – penalties can go from $100/violation to $50K/violation

HITECH/HIPAA Update: 9/23/2013
What Companies that already provide Health Insurance for their employees need to know

• All CEs are required to update all policies and procedures and forms with the updates in HITECH. Changes include:
  – Modification to and addition of certain definitions;
  – Changes in BAAs (final transition 9/23/2014);
  – Requirement for BAs to pass on BA obligations to Subcontractors;
  – Changes in permitting individual access to PHI;
  – Changes in permitting requests for restriction of PHI;
  – Changes in permitting CE to disclose PHI to those involved in an individual’s care;
  – Changes in permitting a CE to use or disclose PHI for marketing;
  – Changes in permitting a CE to use or disclose PHI for fundraising;
  – Changes in the concept of requesting/providing the minimum necessary PHI to accomplish the purpose of the request, use or disclosure;
  – Changes in circumstances in which an authorization is required; and
  – Changes in the identification of breaches of unsecured PHI.
**Employee Health Screenings & Wellness Fairs**

- Have an agreement for the provision of these services that spells out how PHI is going to be handled.
- Have the appropriate disclosures and authorizations in place so that it is clear how or if PHI is going to be disclosed to the employer and for what purpose.

**What Companies May Not Know:**

- Does the company contract with/provide services for any CE (health plan/health care provider/health care clearinghouse)?
- If you provide services to a CE and the CE has to provide you with access to PHI, then you may be a Business Associate (BA) of that CE.
  - Requires you to enter into a BAA with the CE;
  - After HITECH - Requires a BA to comply with various Privacy Standards and Security Standards.

**Is the Company a BA?**

- After the HITECH update it is clear:
  - Even more entities are considered BAs;
  - Many of the HIPAA provisions apply directly to BAs;
  - The enforcement provisions apply to BAs.
- If the Company contracts with CEs, the Company needs to review its contractual relationships to determine if a BA relationship exists.
Is the Company a BA?

• A Business Associate is a “person” who:
  – On behalf of a CE, creates, receives, maintains, or
    transmits PHI for a function or activity regulated by
    the Privacy Standards including:
    • Claims processing or administration;
    • Data analysis, processing or administration;
    • Utilization review;
    • Quality assurance;
    • Patient safety activities;
    • Billing;
    • Benefit management;
    • Practice management; and
    • Repricing . . . OR

Is the Company a BA?

• Provides the following service where that
  service involves the disclosure of PHI from a CE
  or another BA:
  – Legal;
  – Actuarial;
  – Accounting;
  – Consulting;
  – Data aggregation;
  – Management, administrative, accreditation or
    financial services; . . . . OR

Is the Company a BA?

• A Health Information Organization or E-
  Prescribing Gateway
• Other person that provides data transmission
  services with respect to PHI to a CE and that
  requires access on a routine basis to such
  PHI;
• Provider of a Personal Health Record;
• A Subcontractor of a BA
What if the Company is a BA?

- Comply with applicable Privacy and Security Standards:
  - Must enter into a Business Associate Agreement (BAA) and pass on your BA obligations to Subcontractors
  - Develop and implement policies and procedures to comply:
    - Identify when a BA relationship exists
    - Identify when to pass on BA obligations to subcontractors
    - Establish workforce members' responsibilities with the use and disclosure of PHI
    - Establish the minimum necessary PHI to request/access
    - Provide for the rights of the subject of the PHI:
      - Access
      - Amendment
      - Accounting

- Provide safeguards:
  - Administrative; Physical; Technical
  - Sanctions for violations by workforce members
  - Non-retaliation
  - Mitigation of breaches
  - Breach notification
  - Training

Why should Companies care?

- If there is a HIPAA violation there can be both:
  - Criminal Penalties
  - Civil Penalties
HITECH Update: Criminal Penalties

• Amends HIPAA Statute to make it clear that the criminal penalties apply to employees and other individuals, including BAs.

---

HITECH: Civil Money Penalties

• HITECH significantly revises the HIPAA CMP Statute to include non-compliance due to willful neglect and requires DHHS to investigate if a complaint indicates a violation due to willful neglect.
• CMP $ collected to go the OCR and are used for increased enforcement

---

HIPAA Criminal Penalties

• (a) A person who knowingly & in violation of HIPAA:
  • (1) uses or causes to be used a unique health identifier;
  • (2) obtains IIHI relating to an individual; or
  • (3) discloses IIHI to another person, shall be punished as provided in subsection (b) of this section.
• (b) Penalties: A person described above shall--
  • (1) be fined not more than $50,000, imprisoned not more than 1 year, or both;
  • (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
  • (3) if the offense is committed with intent to sell, transfer, or use IIHI for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.
HITECH: Civil Money Penalty Tiers

(a) $100/violation, the total not to exceed $25,000 for identical violations/ calendar year;  
(b) $ 1,000/violation, the total not to exceed $100,000 for identical violations/calendar year;  
(c) $ 10,000/violation, the total not to exceed $250,000 for identical violations/calendar year;  
(d) $ 50,000/violation, the total not to exceed $1,500,000 for identical violations/calendar year.

– A violation where the person did not know and by exercising due diligence would not have known, the penalty will be not less than (a) but not more than (d).

– A violation due to reasonable cause, but not willful neglect, the penalty will be not less than (b) but not more than (d).

– A violation due to willful neglect:
  – If corrected, the penalty will be not less than (c) but not more than (d);
  – If not corrected, the penalty will be not less than (d).

High Risks – Computers and Portable Devices

• Take great care:
  – Risks are high with electronic information
    • Greater access/speed/availability means an even greater risk of potential breaches/liabilities
  – Use of portable devices:
    • Be mindful of where you are using portable devices and whether you have appropriate security (technical and physical)
    • Use only those portable devices that are approved by the Company

CMP for Stolen Mobile Device

• Massachusetts Eye and Ear Infirmary and its associated physician practice
• Self-reported the theft of an unencrypted laptop containing PHI of > 500 patients from an employed physician while on vacation
• No finding of financial or reputational harm to the patients
• Findings: Failure to:
  – Restrict access to PHI from unauthorized users/portable devices and be able to track access
  – Track movement of both Hospital/personal portable devices on and off premises
  – Implement encryption or appropriate alternatives to encryption
• 9/17/2012 – Agreement (3 years)
  – $1.5 Million CMP
  – A Corrective Action Plan (includes a framework for updating policies/procedures and compliance plans for mobile devices)
UPSHOT: WHAT SHOULD A COMPANY DO?
- Newly established health plans – comply with the Privacy and Security Standards
- Established health plans – Update your policies/procedures/practices for HITECH compliance;
- Companies should:
  • Review its contractual relationships with CE clients to determine if a BA relationship exists
  • If a BA relationship exists – establish policies/procedures/practices for HITECH compliance.
- Review their overall risk management strategies:
  • Conduct a risk assessment (privacy and security);
  • Review contracts for risk shifting provisions;
  • Review liability insurance – is a cyber risk policy needed?

QUESTIONS?

Information Privacy and Security
Criminal, Ethical & “Crisis” Issues

December 9, 2013
Will Terpening
Nexsen Pruet, PLLC
704.338.5358 (office)
704.787.3091 (cell/ after hours)
wterpening@nexsenpruet.com
Twitter @WillTerpening
Terpening Practice

- Emergency/crisis response, triage.
  - Privacy "generalist" and compliance resource.
- White collar criminal defense.
  - Pre-indictment negotiations.
  - Trial.
  - Appeal.
- Government/state subpoena response.
- Search warrant response.

CORPORATE CRIMINAL PROBLEMS & INVESTIGATIONS IN DATA PRIVACY

Criminal Enforcement Digital Privacy Tension

Detect, Protect, Prosecute
- How do we prevent and prosecute hacking fraud, data/identity theft cases?
- Need for deterrence.
- Need to try to recover lost proceeds of crimes.

Privacy Rights & Compliance Burden on Corporations
- We want to deter and prosecute these crimes, but costs on complying with federal subpoenas for documents and testimony can be high.
- $/disruptions.
- Privacy rights for clients and corporation need to be considered.
ONE SIDE: NEED TO PREVENT AND PROSECUTE DIGITAL PRIVACY CRIMES


94 These guys seem awesome!
... but their awesomeness cost us $45 million.
... just kidding, they are clearly innocent.


• International conspiracy to withdraw funds from ATMs.
• Sounds techy and sophisticated – but as in all digital crimes, driven and facilitated by human error (on one side) and greed, motivation, opportunity, and savvy on the other.
• Like any other crime, it’s the people, not the technology – and you should prepare for it from that perspective.
ATM Mega Conspiracy: Allegations

Step 1: Overseas hackers target victim financial service providers.
   – Get PINs, account #s, etc.
   – In some instances, change accounts to reflect no withdrawal limit.

ATM Mega Conspiracy: Allegations

Step 2: Hackers then send the stolen data to “a trusted group of associates” (USAO’s words) in U.S., could be anywhere.

ATM Mega Conspiracy: Allegations

Step 3: The “trusted associates” coordinate fraudulent transactions.
   – Their team puts the account info on ATM cards.
   – Large numbers of people use the cards for many ATM transactions.
   – Losses @ $45 million.
Mega Conspiracy Notable Attributes

For some victim banks, relatively low numbers of accounts.
- E.g., for one series of attacks in Dec. 2012, only five accounts were used.
  - But those accounts were used in numerous ATM transactions.
  - And losses were still in millions because the hackers had eliminated withdrawal limits.

When you hear the loss amount, you think of expansive hacking – that is not necessarily so.
- Small data breaches could cause significant harm.

Unlikely to Recover Funds

Indictment (11-12) anticipates difficulty of recovering proceeds:
- Impossible to locate.
- Transferred to third parties, many innocent.
- Placed beyond jurisdiction.
- Significant diminution in value.
  - Dudes in photo squandered their share on first editions of Dickens, an opera season subscription and fine wine.
  - “Substitute assets” probably unavailable.
    - Fraudsters tend not to be savers.

Difficult to Prosecute Organizers

- Perpetrated from outside U.S.
- Difficult to establish hacker identity.
- Which is why you see lower level defendants in EDNY.
- But prosecuting them probably won’t address root problem, or lead to recovery of funds, or even deter current or future ringleaders.
**What Can We Learn & Do?**

Improve technology, sure...
- Frequent PIN changes.
- Separate data in different databases that must be combined for ATM access.
- Unique identifiers like fingerprint identification technology.

But the banks were probably incorporating/developing that.
- And because of tech limitations, concessions to cost and convenience, etc., there will always be risks/gaps.

---

**What to Learn/Do?**

Treat it as a people problem – victim side.
- Perhaps not here, but this kind of exposure often occurs because employees of victim corporations make honest mistakes, or are conspirators in the crime.
- Better compliance controls, training, internal investigations, background checks, etc.
- Educate employees about costs of such disasters.
- Other approaches?

---

**What to Learn/Do?**

People problem – criminal side.
- Emphasize deterrence: both criminal and civil prosecutions – certainty and severity.
- Better allocate limited law enforcement resources.
  - Hold prosecutors/government accountable.
  - Focus public resources on significant crimes, not “low hanging fruit.”
- Better integrate public enforcement authorities with private corporate detection and prevention personnel/resources.
  - But must be truly collaborative, or else becomes a burden on company – as we are about to see!
OTHER SIDE: NEED TO PROTECT PRIVACY RIGHTS & MINIMIZE COMPLIANCE BURDEN ON CORPORATIONS

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause..."

- Fourth Amendment to the United States Constitution

Physical Papers v. Digital Info

- Law treats private emails/data in stored Cloud (e.g., Gmail) very different from private letters stored in a filing cabinet at home.
  - Should it?
  - What do we expect? Do we think of emails like private papers?
- Can seize or demand emails (depending on timing) from third party vendor, leaving owner of emails with little control over production.
- Ramifications for individuals/customers, 3d party vendors, companies that store info with vendors and/or Cloud.
- Implications of giving up control of info in context of demands for production by authorities.
Subpoena v. Warrant

Warrant
- Magistrate screening.
- Particularity – specific time, place, subject, etc.
- Probable cause burden on gvt.
- Less burden on custodian of information.
- Can be more intrusive.

Subpoena
- AUSA simply issues.
- Potential for abuse.
- Can be as broad as prosecutor wants.
- Motion to quash/modify option, but has drawbacks and risks too.
- Burden on company to gather documents, pay for that process.
- See my primer on subpoena and search warrant response.

Subpoena Issues In House
- In many cases, this puts corp. in the difficult position of complying with or moving to quash a subpoena for emails and other private customer data you may possess.
- Protect privacy or tangle with government?
- Particularly problematic for ISP/telecom companies.

Subpoena Compliance Considerations
- Notice to customer whose information was subpoenaed?
- How to protect dissemination once produced; responsibility to do so?
- Costs of search and compliance?
- Adjust data retention policy to store for less time so you won’t have anything to produce (but have to balance with other preservation rules, which vary by industry).
- Need to have policies beforehand governing how to respond and how to communicate with government, customer, and courts.
CLOUD STORAGE MISTAKES & RESPONSES

Cloud Storage Overview

- Corporations are more commonly storing their business data and customer data in 'the cloud.'
- Data previously stored on hard drives or servers controlled by your company is now stored remotely on servers controlled by a vendor.
- Myriad risks of forfeiting that control – when do we cross the line from using cloud as a productive and convenient business tool to a too-risky technology?
- Are there some types of data that are too valuable to keep in the cloud, no matter what precautions you take?
- Your employees use Cloud storage services whether the company knows/permits it or not.

Cloud Storage Overview

- Even such common points of entry like online work email addresses can expose company and customer data if passwords are lost or hacked.
- Personal experience in white collar criminal defense – former employee regularly logging in to retrieve proprietary sales data and potentially provide to competitor.
  - What measures should the company have taken to prevent?
  - And if the data had been sensitive customer info, what would their liability have been?
- Point: It is not the case that you only have exposure if you are using the Cloud wholesale, for all your data – these are issues even if you have web-based email (or even handheld-device based email), etc.
Cloud Summary - Pros

- Convenience – allows employees to collaborate remotely and in real time.
- Litigation benefits – for instance, makes it easier for you to share discovery and work product with your outside counsel.
- Stability – in some instances, particularly for smaller companies with less sophisticated IT operations, may be more stable and reliable.

Cloud Summary - Risks

- You relinquish control to a vendor, meaning:
  - Potentially additional personnel with access to sensitive data (on vendor side).
  - A lot is riding on a password.
  - You inherit the vendor’s security mistakes (i.e., if they have a leak, you do).
  - What happens when regulators, prosecutors, or others subpoena your documents from the vendor?

Dropbox & Evernote Functionality

- Dropbox (and the many services like it): Users create a folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files in Cloud and on computer.
- Evernote: Lets you take notes that are automatically uploaded to Cloud and synched across your computers and handheld devices; increasingly used in corporate context.
Serial Dropbox Mistakes

- June 20, 2011: all Dropbox accounts could be accessed without password for 4 hours.
- Still widely used and popular – "world's fifth most valuable web startup."
  - In other words, Dropbox and other services are not going away as an issue for companies to have to deal with from legal and other perspectives.

Evernote Incident

- March 2, 2013: Evernote reveals that hackers gained access to their network and been able to access user information, including usernames, email addresses, and encrypted passwords.
- All users asked to reset their passwords.
- Evernote accelerates plans to implement an optional two-factor authentication option for all users.
- Problem: Many of your company's employees are storing work passwords, proprietary notes, and other company materials on Evernote and similar services.

Lessons

- How to help your company address similar data leaks (and how to prepare a front-end plan) – what not to do.
- How to take precautions before using Cloud data services.
- Potential reasons to restrict employee use of services like Evernote to contain company information.
- Your company needs clear guidelines about what types of info it will/ would never store in cloud.
  - E.g., certain types of information it would want to control better than it could if subpoenaed from third party storage vendor by authorities: highly sensitive customer data, key proprietary information and trade secrets.
Dropbox & Evernote Disclosure Errors

• Both companies widely criticized for how they disclosed and followed up with customers on the leaks.
• Can be used as case studies – lessons for what to do/ not to do if your company faces similar data breaches.

Dropbox Disclosure

"Hi Dropboxers,

Yesterday we made a code update at 1:54pm Pacific time that introduced a bug affecting our authentication mechanism. We discovered this at 5:41pm and a fix was live at 5:46pm. A very small number of users (much less than 1 percent) logged in during that period, some of whom could have logged into an account without the correct password. As a precaution, we ended all logged in sessions. We're conducting a thorough investigation of related activity to understand whether any accounts were improperly accessed. If we identify any specific instances of unusual activity, we'll immediately notify the account owner. If you're concerned about any activity that has occurred in your account, you can contact us at support@dropbox.com.

This should never have happened. We are scrutinizing our controls and we will be implementing additional safeguards to prevent this from happening again."

• Litigation issues.

Disclosure Analysis

• Handling PR well = litigation risk mitigation.
• Problems here?
  – Formality?
  – No hotline to call?
  – Doesn’t explain why it took them 4 hours to detect.
• Positives?
  – Taking matter seriously/ investigation plan.
  – Promise to contact small number of affected users directly.
  – Emphasize small number of users.
  – Quick fix once discovered.
Lessons Learned

- If your company maintains its or its customers’ data in the Cloud, select your vendors carefully.
- You, as in-house counsel, should carefully work with your IT staff to “ask vendors the right questions.”
- Address consequences of leak in compliance plan – have a plan ahead of time.
- Do not minimize or delay dialogue with customers if their data is compromised – for both business and legal reasons.

Cloud Storage and Government Subpoenas

- Another risk of cloud storage for your customer’s data or allowing outside counsel to store your company’s data in Cloud.
- Vendor obligations to comply with federal subpoenas for your information.
- You have less control.
- Determine vendor’s procedure for subpoena response first?
  - E.g., can vendor access the information, notice and objection process, past vendor responses to other customers’ subpoenas?
  - Also a potential issue in private civil litigation.

Litigation Prevention/Mitigation

Preventative End-User Measures to Include:

- Data encryption before data sent to Cloud.
- Sophisticated and often-changed passwords (including dual logins).
- Notify customers/clients that data is stored in this fashion as part of contracts governing basic relationship.
- Be aware of industry-specific rules with additional restrictions on electronic data storage (e.g., FINRA/securities, or medical industries).
- Address Cloud storage issues (and leak response plan) in compliance plan.
Litigation Prevention

• Post-Leak:
  • Immediate internal investigation.
  • Retain outside counsel – privilege/ work product issues.
  • Interview key personnel.
  • Document measures taken.
• Immediately and fully notify customers.
  • No cover up, minimization, or delayed reporting.
  • Include plan/potential compensation offer.
  • Hotline for customers.

American Bar Association & Other Guidance

ETHICS & LAW OF CLOUD STORAGE

ABA and NC Ethics

Relevance to in-house attorneys:
1. Need to understand minimal obligations governing how outside counsel you hire protect your client’s (your company’s) data once you give it to them.
2. Need to know enough to instruct (if necessary) outside counsel to take more robust protective measures to protect electronic data in cloud or elsewhere.
3. ABA and Bar Ethics opinions provide analysis that can help you shape your own company’s protocols for storing and protecting customer and other sensitive data.
ABA on Cloud Issues


ABA

New Rule 1.6(c) governing inadvertent disclosure protects lawyers who make “reasonable efforts” to avoid disclosure. Commentary to new Rule subsection: “The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).”

ABA Position: In-House Counsel Implications

- Because of convenience and tacit ABA encouragement, more outside counsel will store your company’s data in the cloud.
- Baseline “reasonableness” standard is forgiving to outside counsel.
- Guidance to outside counsel is generic and unspecific.
- It is your responsibility to protect your company from the serious consequences of data breaches, involving your info, by outside counsel.
N.C. Rules of Professional Conduct

- Cloud storage for client data permitted.
- “Reasonable care” standard of protection.
- Specific NC recommendations:
  - Review terms and policies, and if necessary renegotiate, to ensure they’re consistent with ethical obligations.
  - Evaluate vendor’s security measures and backup strategy.
  - Ensure data can be retrieved if vendor shuts down or lawyer wishes to cancel service.

N.C. Rules

  - “A lawyer may contract with a vendor of software as a service provided the lawyer uses reasonable care to safeguard confidential client information.”
- NB – these standards (including whether Cloud storage of client data is permitted and standard of care) vary from state to state.

2011 Formal Ethics Opinion 6

- “[L]aw firms may involve the storage of a law firm’s data, including client files… and work product, on remote servers rather than on the law firm’s own computer and, therefore, outside the direct control of the firm’s lawyers.”
- “Lawyers have duties to safeguard confidential client information, including:
  - protecting that information from unauthorized disclosure, and
  - [protecting] client property from destruction, degradation, or loss (whether from system failure, natural disaster, or dissolution of a vendor’s business)."
Ethics Opinion 6

Lawyers Must Take Measures Including the Following:

• RPC 1.6: a lawyer may not reveal information acquired during the professional relationship with a client unless the client gives informed consent or the disclosure is impliedly authorized to carry out the representation.

• When transmitting confidential client information, a lawyer must take “reasonable precautions to prevent the information from coming into the hands of unintended recipients.”

• “This obligation does not require that a lawyer use only infallibly secure methods of communication,” and allows lawyers to store data with outside vendors.

Ethics Opinion

• The lawyer must protect against security weaknesses unique to the internet, particularly “end-user” vulnerabilities found in the lawyer’s own law office.

Ethics Opinion

“Are there measures that a lawyer or law firm should consider when assessing a… vendor or seeking to minimize the security risks…?“

“This opinion does not set forth specific security requirements because mandatory security measures would create a false sense of security in an environment where the risks are continually changing. Instead, due diligence and frequent and regular education are required.”
Ethics Opinion: Recommended Measures

- An agreement on how the vendor will handle confidential client information in keeping with the lawyer’s professional responsibilities.
- The law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor’s software or source code.
- Vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.
- Careful review of the terms of the law firm’s user or license agreement including the security policy.
- Evaluation of vendor’s (or any third party data hosting company’s) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.

You can’t spell PRIVACY without “IP”

By Corky Klett
© 2013 Nexsen Pruet LLC

Privacy

Arises out of Constitution

- 1st Amendment - Protection of personal liberties
- 3rd Amendment - No quartering of soldiers in private homes
- 4th Amendment - Warrantless/Unreasonable searches – expectation of privacy
- 5th Amendment - Criminal suspect may keep incriminating evidence secret
- 14th Amendment - Prevents States from denying citizens fundamental rights
### Invasion of Privacy

- **Physical Intrusion** - Trespass
- **Non-Physical Intrusion** - Wiretaps, Microphone, Video
- Must be considered “highly offensive” to reasonable person
- No expectation of privacy in public matters - Mug shots, paparazzi in public

### Public Disclosure of Private Facts

Unlike Libel/Slander/Defamation – **Liability for truthful publicity must be**:

- Sufficiently private or not in public domain
- Sufficiently intimate
- Highly offensive to reasonable person

Limited Protection for Business:

Overriding commercial free speech interests

### False Light Publicity

- Protect individuals from public disclosure of false information about reputation/beliefs/activities
- Need not be private or defamatory
- Elements:
  1. Portrayal must be highly offensive to reasonable person
  2. Actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed
- Different from libel:
  1. No need to prove injury or damage to reputation, only that statement “highly offensive”
Misappropriation of Name/Likeness/Image/Persona

- Individuals have exclusive property rights in their identity
- Non-consensual commercial appropriation
- Defense – news gathering, fair use

No "Privacy Rights" for Corporations

- Supreme Court Decision: *FCC v. AT&T*
  - AT&T sought to take advantage of "personal privacy" exemption under FOIA
  - Held: "personal privacy" applies to interests of individuals, not corporations

Businesses Do Have “Privacy” Interests in Trade Secrets

- Misappropriation of Proprietary Information
- Must be commercially valuable
- Must be kept secret/private
Misappropriation of Name/Likeness/Image/Persona

- For Business:
  - Trademark Infringement
  - Unfair Competition (Lanham Act)
  - False Advertising

Thank you

Corky Klett
wklett@nexsenpruet.com
© 2013 Nexsen Pruet LLC