How we got to where we are today on privacy and security law

Kirk J. Nahra
Wiley Rein LLP
Washington, D.C.
202.719.7335
KNahra@wileyrein.com

What I'll be covering

- A brief introduction to some of the key topics for the program
- A bit of a summary of how we got to where we are today on privacy and security law
- Highlights of some of the key issues affecting privacy and security law today
- Raise some issues to think about over the conference

The Old Days

- Privacy was an issue about the government and the individual
- Arose in contexts like abortion, membership in controversial organizations, birth control
- Not an issue in the commercial context
- 9/11 revived the “individual vs the government” component of the privacy debate (which continues today)

Today

- Privacy is much more than a question of individual rights versus the government
- A recognized right/duty/obligation in many commercial relationships – individuals have certain "rights" or "expectations" about their information in commercial settings
- Often driven by specific events (e.g., video rentals and drivers license information)
- Becoming a universal issue, applicable in some way to most personal information held by businesses about customers, employees and others
- Security also becoming a legal issue rather than a best practice

What Is Driving Privacy As A Big Issue?

- Internet as a source and distributor of information
- Consolidation of the financial services industry
- Increasing uses and sensitivity of medical information
- Bigger and bigger computerized databases
- Newest issue – security breaches and identity theft

Hot topics – Identity Theft

- Ongoing risks and concerns
- Recent GAO Report – Lots of breaches, few identifiable incidents of identity theft from these breaches
- Recent report from the DOJ/FTC Identity Theft Task Force – Required reading for anyone interested in the issue

Medical Identity Theft

- Major study (May 2006) http://www.worldprivacyforum.org/medicalidentitytheft.html.
- Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity – such as insurance information -- without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods.
- Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name

World Privacy Forum Report

- Aside from normal elements of fraud, victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. They may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them.
- Medical identity theft is largely a crime that is perpetrated by trusted insiders.

The Cleveland Clinic Case

- Makes the connection between identity theft and health care fraud
- Indictment of a former Cleveland Clinic Florida employee for conspiracy to commit health care fraud with personal information of more than 1,100 Naples patients
- Patient information provided to outsider, who then fabricated Medicare claims

Enforcement

- Government enforcement increasing, but still very limited
- Essentially no HIPAA Enforcement
- Very limited GLB enforcement
- Some FTC enforcement related to security breach issues
- Limited enforcement in other settings (e.g., Do Not Call, COPPA, CAN-SPAM)

Enforcement Issues

- Is the enforcement environment likely to be changing?
- Is the lack of visible enforcement an actual problem?
- Evaluate what your company is doing to guard against “Privacy-creep” – a lessening of standards related to a lack of enforcement.

Compare/contrast

- Nationwide Building Society in England (NOT Nationwide Insurance) – stolen laptop
- Company's systems and controls should have been robust enough to anticipate equipment theft or loss and to reduce the risk of sensitive data being compromised as a result of such a loss
- Fined almost $2 million dollars

Notification and mitigation

- Important new element to the security/privacy breach debate
- Astonishing number of media reports about large and small security breaches, almost daily occurrences, affecting all industries
- Has led to state laws – in more than 35 states – about notification of individuals in the event of a security breach
- Likelihood of new federal legislation (is it still likely?)

Mitigation

- Mitigation involves:
  1. Identifying the problem
  2. Determining the cause of the problem
  3. Evaluating any potential harm from the problem
  4. Stopping the bleeding from the problem
  5. Evaluating appropriate changes (if any)
  6. Determining any other legally required steps (or appropriate business steps)
  7. Does mitigation or specific law require notification to individuals?

Issues for consideration

- Are the notice standards reasonable?
- Are they useful and practical?
- Do these notices help anyone?
- Does notice serve a real purpose beyond publicizing security breaches?
- Are the notice rules pushing companies (and their vendors) to higher standards?
- Don’t forget mitigation, even when notification is not required.

Overall status on litigation

- Increasing awareness of privacy and security issues in litigation
- Volume of privacy-related litigation has been small, but steadily increasing
- Wide range of litigation related to security breaches and identity theft
- Courts have been skeptical of many claims
- Is a breakthrough case on the horizon?
- Is “negligence” a viable theory?

Why Hasn't There been More Litigation?

- Typically, there has been no private cause of action in most privacy statutes or regulations (e.g., HIPAA, GLB)
- Substantial difficulties with proof of damages (both as an incentive to bring cases and as an element of a claim that can survive a motion to dismiss)
- Limited government enforcement as a stepping stone to class litigation

The state of the play today

- Increasing enforcement activity (but still limited)
- Widespread publicity surrounding security breach incidents
- Potential harm related to identity theft (although GAO reports that most breaches do not lead to identity theft)
- Some “corporate vs. corporate” cases
- Continuing difficulties in finding “class” cases
- Limited situations involving individual harm
- Plaintiffs still struggling with “square peg and round hole” problem

Damages are a real hurdle

- Smith v. Chase Manhattan Bank
- Financial institution gave list to third party, received payments on sales
- Said it didn't do these things in privacy notice
- No damages alleged/no cause of action
- Only unwanted telemarketing

Litigation challenge

- How do you get around the fact that there often is no private cause of action?
- The HIPAA example
- We know there is no HIPAA cause of action
- We're starting to see breach of confidentiality claims that are called things other than HIPAA
- We're starting to see HIPAA emerge as a "standard of care" that can be breached

Sorensen v. Barbuto (Utah)

- Doctor provided information to defense attorneys in a case brought by the doctor's former patient. While the Court dismissed breach of contract claims against the doctor, the appeals court allowed a claim to proceed for "a breach of the physician's fiduciary duty of confidentiality."

Herman v. Kratche (Ohio Ct. App.)

- Plaintiff received medical treatment from a clinic. Results of the treatment were sent to the HR Department of plaintiff's employer
- Clinic was told that there was no workers comp. claim, and that nothing should be provided to employer – material continued to be sent.
- Court says that clinic had a fiduciary duty to patient to keep information confidential and breached that duty.

Acosta v. Bynum (N.C. Ct. App.)

- Court reinstated a claim for intentional infliction of emotional distress against a psychiatrist who allegedly allowed an officer manager access to psychiatric records that were then used to cause harm to a patient.
- The complaint references HIPAA as creating a standard of care for the defendant.
- The trial court had dismissed the claim, in part because HIPAA does not create a private cause of action.
- The appellate court reversed, not because HIPAA creates a private cause of action, but because they found it appropriate to use HIPAA as creating a standard of care in making claims that a defendant violated a standard of care.

Some thoughts

- In situations involving individuals and specific bad behavior, courts may stretch to find a cause of action.
- This has not extended so far to class actions
- Plaintiffs' lawyers are being creative (and with some success) in individual harm cases.

Litigation trouble spots.

- Preemption – continued confusion
- The Georgia Supreme Court, in *Allen v. Wright*, held that the HIPAA Privacy Rule preempted Georgia's 2005 tort reform statute requiring malpractice plaintiffs to file with their complaints a "medical authorization form" enabling the defendants' attorneys to obtain and disclose protected health information to facilitate their defense of the plaintiff's claims.
- Theory was that entire statute was preempted because the required authorization didn’t meet HIPAA standards.

Struggles with "required by law"

- In State ex rel. Cincinnati Enquirer v. Daniels, (2006), the Ohio Supreme Court, in dicta, indicated that the State Freedom of Information laws trumped the HIPAA Privacy Rule, so that information held by the state, to the extent it had a HIPAA covered entity role, also would be subject to disclosure under the freedom of information act.

Required by law

- Reporter requested statistical information regarding allegations of abuse and subsequent investigations of abuse in state mental facilities.
- Department refused to produce based on HIPAA
- Court assumed that information was covered by HIPAA, and that Department was a covered entity, and then said that information should be produced, because it was required by the open records law to be produced.

Big News – The FACTA Suits

- Huge number of potential class action lawsuits brought against merchants based on truncation of credit card numbers and printing of expiration dates
- Class action firms are seeking huge statutory damages based on alleged "willful" violation
- All kinds of companies are getting sued
- What will these suits do to the overall environment?

Security breach cases

- Becoming more and more routine, in large scale breaches
- Plaintiffs' class action lawyers jumping on the bandwagon
- Plaintiffs typically are potentially injured consumers along with shareholder types
- No "breakthrough" case yet

Corporate v. corporate cases

- Three state banking associations filed a federal class action complaint alleging that TJX Cos. Inc. should pay them damages because it engaged in unfair trade practices and deceptive acts by failing to implement reasonable data security measures to prevent the massive breach of payment card data by the retailer.
- Similar cases filed against BJ's Wholesale
- Most have been unsuccessful

Electronic health records

- A significant new development in and out of the health care industry
- The marketplace is moving quickly
- Can the regulatory system keep up?
- Can we achieve the right balance between protecting privacy and security interests while still achieving important public policy goals?

Wall Street Journal

- "As the health care industry embraces electronic recordkeeping, millions of pages of old documents are being scanned into computers across the country. The goal is to make patient records more complete and readily available for diagnosis, treatment and claims-payment purposes. But the move has kindled patient concern about who might gain access to sensitive medical files – data that now can be transmitted with the click of a computer mouse."

Perspectives

- GAO – “As the use of electronic health information exchange increases, so does the need to protect personal health information from inappropriate disclosure.”
- True?
- Why does this “increase” need “increased” protection?
- Are they talking about privacy or security?

Perspectives

- GAO - “The capacity of health information exchange organizations to store and manage a large amount of electronic health information increases the risk that a breach in security could expose the personal health information of numerous individuals.”
- True? Does “bigger” mean more risk? Is it this “exchange” function that makes this environment different?

Information Security

- Security is now a separate legal requirement – connected to privacy but with different rules and issues
- Security is a top issue today, with almost daily news stories and a tie to identity theft
- Security has moved from a business-driven "best practice" to a legal requirement in essentially all industries.
- Visible and public breaches on a relatively consistent basis

Issues to consider

- Is a requirement to have “reasonable and appropriate” security practices a meaningful requirement?
- How do companies deal with the uncertainty of knowing that “reasonable” practices won’t always work?
- Will the government enforcement agencies be able to evaluate “reasonableness” where there are actual breaches? (Note the recent “breach” involving a government health care contractor – where the “breach” was sending health care files over an unencrypted channel.)

Vendor Issues

- Most privacy and security laws require contractual provisions related to privacy and security
- A specific requirement for any contracts with the health care industry or the financial services industry
- Applies to most companies as both “principal” and “agent” (or vendor)
- All companies must understand how these laws apply to them and to their vendors and their customers
- Appropriate vendor management is an enormous issue
- Are the legal standards appropriate?