PAI PRIVACY ASSOCIATES INTERNATIONAL LLC

Maintaining Privacy Policies and Responding to Security Breaches

6th Annual Information Technology Law Seminar

September 25, 2013

Keith A. Cheresko Principal,
Privacy Associates International LLC

Purpose

- Explore privacy policy creation and maintenance
- Shed light on preparing for and responding to data breaches.
- Review common elements in data breach policies and procedures
- Provide actionable ideas to help increase the security for data under your control

What is Privacy?

- Different meanings to different people
- Large element cultural
- Hundreds of definitions, but most involve the ability of a person to control information about herself, or access to herself

Information Privacy

- A category of privacy rights
- Importance has been magnified by the Information Technology revolution and economic globalization
- Relates to the interest a person has in controlling his or her personal information
- Relevant to all organizations that handle personal information
- Applicable rules differ, but some basic concepts are the same

PAI

Terminology

Personal -

“of, relating to, or affecting a particular person: private, individual <personal ambition> <personal financial gain>” *Webster*

Personal Information (PI) -

data of, relating to, or affecting a particular person

Personally identifiable Information (PII) -

data that can be tied to a unique person some of which has obtain defined legal protection (information relating to an identified or identifiable individual)

Privacy vs. Security

- Privacy laws focus on the collection, use, and disclosure of personal information
- Security is the means by which we safeguard information against unauthorized acquisition, use, disclosure, alteration, destruction
- Security is necessary to maintain privacy, but . . .
  - Security alone will not maintain privacy (e.g., notice, consent, retention)
  - Security may conflict with privacy (e.g., national security, employee monitoring)

Privacy Statements

- Privacy statements are a typical way of giving notice to individuals as to how their personal information will be used
- Originally furnished by merchants for competitive reasons, now required by various US laws
- US Federal Trade Commission has been extremely active in this area

Privacy Statements

- Critical that the privacy statement reflects what is ***actually*** done, not what someone thinks looks good or ***thinks*** is being done
- If cookies or other tracking technologies are placed on web-based forms, that should be disclosed
- Planned disclosures to third parties and the purposes of collection should be included
- All the technical complexity can be boiled down to one simple statement

SAY WHAT YOU DO

AND

DO WHAT YOU SAY

KNOW WHAT YOU DO

Privacy Statements

- To know “what you do” involves work
- Conduct inventory of PI - establish a data map
- Maintain the accuracy of the data map
- Privacy Risk Assessment determine security risks to PI

Types of Privacy Statements

- Long form
- Short form
- Layered
- Just in time

Content of Privacy Statements

- Content varies
- Based on Fair Information Practice Principals (FIPPs)
  - Notice/Awareness
  - Choice/Consent
  - Access/Participation
  - Integrity/Security
  - Enforcement/Redress

Content of Privacy Statements

- Identification of : entity collecting the data, uses to which the data will be put , potential recipients of the data.
- The nature of the data collected and the means by which it is collected
- Whether provision of requested data is voluntary or required and consequences of refusal to provide

Content of Privacy Statements

- Steps taken to ensure the confidentiality, integrity and quality of data
- Effective date of the privacy statement
- Other factors – COPPA, State Law, Links
- Reservation of right to amend and how it will work

Content of Privacy Statements

- If you decide to change your stated practices:
  - The purposes of collection change, or
  - You decide to make the information available to third parties not included in the original statement (e.g. the public)

  You must go back and give the data subjects the choice not to have their data included
- Prudent to include a statement to address effect of take over and bankruptcy of the existing entity and how personal information may be transferred

US Federal Trade Commission

- FTC Act prohibits “unfair or deceptive acts or practices in commerce and FTC *actively* uses it powers
- “Deception” theory: the entity didn’t do what it said it would do
- “Unfairness” theory: the promise doesn’t matter, simply unfair not to protect consumer personal information
- Responsibility for the acts of your contractors and suppliers

FTC and Consumer Data

- FTC does not expect maximum available security
- Security should be reasonable and appropriate to:
  - Organization's size and complexity
  - The nature and scope of its activities
  - Sensitivity of the PI
- Privacy risk assessments should be conducted to determine areas of greatest risk and areas in which a breach would have the most serious consequences
- Reasonable safeguards must be implemented in light of those findings.

FTC Does Expect Reasonable and Appropriate Security for PI

Physical Security includes

- Facility access controls
- Safeguarding hard copy documents with PI
- Securing hardware on which PI is stored

FTC Does Expect Reasonable and Appropriate Security for PI

Technical Security relates to the protection of electronic information through methods including:

- Firewalls
- Anti-spyware programs
- Encryption
- De-identification applications
- System scanning

FTC Does Expect Reasonable and Appropriate Security for PI

Administrative Security includes rules and training applicable to PI handling such as:

- Ensuring access authorization is only given to individuals with legitimate purposes
- Authentication rules
- Rules limiting what data can be stored on portable devices such as laptops and thumb drives
- Security provisions in supplier contracts
- Security training for those with access to PI

Process Approach to Security

- Emerging process orientation to data security
  - Must be able to evidence that you have examined various security risks and have put into place reasonable safeguards to address those risks
  - Safeguards need not be the maximum level of security, but must be proportionate to the risk – i.e. a cost benefit analysis
  - Even if a breach subsequently occurs, a properly documented analysis of risks and responses will help immensely in a challenge situation

What To Do About Security Risks

- Best advice: keep personal data absolutely secure from all possible threats at all times so no breach could ever occur
- Next best advice -- make certain:
  - reasonable administrative, technical and physical security measures are in place and documented, in line with analysis of risks
  - contracts with outside suppliers that handle personal information have appropriate security language, including notification and cooperation provisions
  - you have systems and processes to discover or become informed of a breach
  - You have a well thought out process involving the right people to respond quickly and decisively to a breach

Statistics

As of August 28, Privacy Clearing House database lists:

- 609,069,423 records from 3871 data breaches made public from 2005 to August 2013
- 1,796,027 records in their database from 313 breaches made public so far in 2013
- 155,366 records in database from 19 breaches made public in August alone with nearly half reporting “unknown” amounts

http://www.privacyrights.org/data-breach/new

Statistics

The Verizon 2013 Data Breach Investigations Report provides analysis of:

47,000+ reported incidents and

621 confirmed data breaches

Statistics

The Ponemon Institute’s *2013 Cost of Data Breach Study* for US-based companies reports:

$ 188 the average cost per compromised record and

$5,400,000 average in organizational costs per event

“[S]ome organizations will be a target **regardless** of what they do, but most become a target **because** of what they do or don’t do). If your organization is indeed a target of choice, understand as much as you can about what your opponent is likely to do and how far they are willing to go. The rest of us should work to eliminate sloppy configurations, needless services, and exposed vulnerabilities that inevitably bring unwanted attention.”

-2013 DBIR, p 48

Is a Privacy Breach Different than a Security Breach?

PAI

Privacy vs. Security

- To answer, first consider the difference between privacy and security
- Privacy relates to giving an individual some level of control over his personally identifiable information (PII)
  - Definitions of PII vary, which we will discuss later
  - To give the individual some control, privacy is concerned with matters such as choice, notice, access, data quality, and security ***as it relates to PII***
- Data security is concerned with the safeguarding of all data, not just PII
- Privacy broader than security in one sense, security broader than privacy in another sense

What is a Privacy Breach?

Can relate to two situations:

- The ***unauthorized access to or acquisition of*** the kind of PII specified by an applicable law (security of PII)
- The failure to live up to obligations made with respect to non-security related aspects of privacy (notice, choice, access, etc.)

What is a Security Breach?

The unauthorized access to or acquisition of anything proprietary:

Buildings, facilities other physical plants,
Computer equipment
Product Inventory
Confidential or secret information
Trade secrets
Intellectual property
Proprietary items
Financial information
Data in paper or electronic data
Personal information of consumers, employees, etc.
Customers lists

Be Prepared

Taking the steps necessary to minimize potential security incidents from occurring is a good first step any response preparation process. And while prevention efforts are important, actual preparation, including a well-designed, practiced, and tested response plan, is an essential tool for mitigating the financial, legal and reputational harm associated with a security incident. Regardless of how a breach begins, an organization's initial response is key to help minimize harm to affected people and your organization. Have a written breach response plan ready and tested ***before*** a breach happens.

Causes of Data Breaches

- Lost or stolen laptops, removable storage devices or paper recordings containing personal information
- Inappropriate disposal of hard drives and digital storage media (without contents being erased)
- Hacking of databases containing personal information
- Paper records being taken from insecure recycling or garbage bins
- Trusted insiders with access who abuse rights
- Others

Consequences of a breach?

Depending on the nature, sensitivity, type and volume of data or other assets compromised it may mean

- Lost business and Operating inefficiencies
- Organizational freeze up & Increased costs
- Adverse impact on market valuation
- Potential ID theft & Adverse labor consequences.

Breach Notification Laws

- Designed to help enforce security obligations
  - In theory helps consumers protect themselves
  - Provides government authorities enforcement opportunities
  - Bad PR and breach-associated costs encourage compliance
- In 46 states and also at the federal level
- Michigan Identity Theft Protection Act

Breach Notification Laws

- Breaches generally triggered by the unauthorized access to, or acquisition of, PII covered by the law
- Other variables affect whether a breach notification law applies such as:
  - Storage medium involved
  - Use of data encryption

Individualized Approach

- Each company is different in terms of culture, degree of centralization, and other factors that affect data breach preparations
- Many different ways to achieve the desired result: no “right” answer
- Whatever the process, in the chaos of a large data breach having an airline pilot-like checklist to systematically review is extremely comforting

PAI

Preparations for an incident

- Obtaining Senior Management support/sponsor
- Creating a written Incident Response (IR)Plan
- Selecting and training an IR Team
- Retaining necessary service providers
- Testing the IR plan *before* you use it
- Keeping your fingers crossed you'll avoid needing to use the IRP

Incident Prep Challenges

- Lack of written IR plan, training and testing
- Employees
  - Often do not recognize a data breach when they see it
  - Do not know what to do about it
  - May not have a sense of urgency
  - Do not appreciate the potential consequences

Breach Incident Processing

- Assemble the team and dust off the plan
- Stop the bleeding
- Determine the injury
- Involve those with whom prior arrangements were made as necessary
- Notify as required in an appropriate manner
- Report to authorities as required
- Document actions and reasons for them
- Fix the concern
- Evaluate and revise as necessary

Team Composition and Activation

A core team that is common to all incidents

- Maintains corporate history
- Develops necessary know-how and assures consistence
- Gains experience to appropriately modify existing policies and procedures
- Is kept up to date on major legal changes

Team Composition and Activation

Advantages of a two-level approach

- Can include subject matter experts and employees closest to the facts directly in meetings – minimize hearsay situations
- A data breach incident can be a full-time job for many individuals – putting certain communications, record-keeping and other administrative responsibilities on the business unit with most responsibility for the incident allows core team members to do their day jobs
- Often a senior executive from the business unit or staff involved who is not part of the working level incident team is designated as the Decision-Maker.
- The Decision-Maker makes the high-level calls on matters such as what will be done for individuals whose data was involved in the breach, how to deal with budget issues, obtaining any necessary approvals from relevant corporate committees, etc.

Team Composition and Activation

- Communications among team members is critical
- Need an individual and alternatives to act as an initial communication hub once notice of incident has come in
- Depending on initial view of possible size and importance of breach, the call for a meeting should be a "drop everything" event and take place in a matter of hours, not days
- Critical for each committee member to have current lists (online-offline) of home phone/cell and other contact info for non-business hour events
- To the extent that one cannot use its in-house recourses, vendors for call centers, printing and mailing, and similar needs should be arranged before any breach occurs

Breach Incident Processing

According to Regulatory advice in the event of an incident do:

- Immediately isolate affected systems to prevent further intrusion loss of data or other damage
- Email traffic may be monitored; Use the telephone or other reasonably secure means to communicate (VOIP?)
- Notify law enforcement
- Activate all auditing software if not already activated
- Preserve pertinent system logs
- Make backup copies of damages or altered files and keep them securely
- Identify where affected system resides in network topology
- Identify all systems and agencies that connect to affected system
- Identify programs and processes that operate on the affected system, impact of the disruption and max allowable outage time
- If necessary make arrangements for continuity of services

Don’t delete, move or alter files, contact suspected perp., or do forensic analysis

Initial Diagnosis

- It is unusual to have all the correct facts immediately upon receipt of notice of an incident
- Need to collect all possible facts and based on those, preliminarily identify internal and external stakeholders
- Ask the 5 W questions – “who, what, where, when, why” + “how”

Initial Diagnosis

- Based on available facts, should further investigation be done under direction of counsel to try to obtain work product privilege rather than under direction of the IRT?
- Commence record-keeping protocol
  - Critical for possible future liability purposes to keep a contemporaneous record of what information the company had when, and what decisions were taken as a result
  - Use of standardized event logs and decision logs makes the process easier

Initial Diagnosis

Draft initial write-up of “what happened” based on knowledge to date

- Will be required to communicate to internal and external stakeholders
- Will be continually revised as facts develop/change
- A single official version mandatorily used for all purposes will help assure accuracy and avoid expensive and embarrassing inconsistencies

Initial Diagnosis

- Determine and mitigate possible adverse action by data subjects or other stakeholders
- Will notice to affected data subjects possibly be legally required? If so what are the rules, time limits, forms, etc.
- Will notice to affected data subjects possibly be required for business reasons even if not legally required? If so, is it clear who will make the decision?
- Do you require additional resources to deal with the situation? Forensic or technical experts? Outside counsel?

Containment

- The exact actions that can be taken in this phase are unique to each incident and very fact-specific
- Important to avoid group responsibilities for tasks and to be specific as to who, what, why, how and when:
  - Assignments should be included in event log and a verification of completion mechanism designed
  - Review updated template notification letters on the websites of the privacy officials in potentially affected jurisdictions
- To the extent a supplier is involved, a close working relationship coordinated by an appropriate individual should be established, if at all possible, to avoid "surprises"

Continuing Actions

Again, this phase is very fact specific

- Continue to update fact and decision logs, “What Happened” explanation
- Gage public/government reaction if news has broken
- Prepare individual and governmental notices if required
  - Note letters must be specific enough to meet sometime conflicting state law requirements
  - Letters must not be so specific as to alert the laptop thief that he has something more valuable than the laptop
  - Entire IRT should approve or suggest modifications

Continuing Actions

- Prepare to deal with the resulting communications issues
  - Customers wanting more info
  - Law enforcement
  - Media
  - FTC
  - SEC
  - Credit bureaus
  - State AGs
  - Executives, retail outlets and business partners
- Write call center scripts and do necessary training – either for holding statement or notification follow-ups

Resolution

- Send notifications as required
- Prepare constituencies to deal with the stakeholders
- Continue to update all logs under record-keeping protocol
- Identify and assign responsibility for any additional actions that have to be resolved

Closing

- Close out logs, determine if Final Report useful
- Document lessons learned and share with appropriate stakeholders
- Assign one or more members to follow-up on recommended changes

Contact Information

Keith A. Cheresko

Privacy Associates International LLC

kcheresko@privassoc.com

www.privassoc.com

(248) 535-2819