PRIVACY ASSOCIATES INTERNATIONAL LLC

Privacy Statements

SBM IT Law Section

Privacy Committee

October 20, 2016

Keith A. Cheresko, Principal Robert L. Rothman, Principal

Privacy Associates International LLC

Purpose of Presentation

- Explore Privacy Statements: why entities create them, what is normally covered, applicable law, specialized statements
- Get input and thoughts from all Privacy Committee members

Terms

- Privacy Policy

  One or more internal dictates by an entity normally addressed to employees and agents setting forth how and what personal information should be collected, maintained, used and shared

- Privacy Statement

  A notice aimed at one or more categories of data subjects or potential data subjects explaining how their personal information will be collected, maintained, used and shared by an entity together with a communication of data subject rights in connection therewith

Typical Internal Privacy Policies

- Handling of Consumer Information
- Handling of Employee Information
- Handling of Shareholder Information
- Handling of Vendor Information
- Types of information that can and cannot be stored on laptops or other portable media
- Social media policy
- Information Security Policy

Privacy Statements

- "Say what you do, do what you say, "
  - Statements must reflect ***actual*** handling of personal information by the entity: not what some other company put in its statement or some aspirational state
  - Enforcement for fibbing
- Learning how an entity is actually handling personal information is often the most challenging part of writing a privacy statement
- If in the course of writing a privacy statement, an entity determines it is not handling personal information properly, or competitively, that situation should be addressed before a privacy statement is finalized

PAI

Form of Privacy Statements

- Vary greatly: advantages and disadvantages to various approaches
- Multi-page legalese form
  - May (or may not) best protect entity from legal standpoint
  - May not be well received by data subjects
  - Makes the lawyers sleep better
- Simple consumer-friendly form
  - May not lend itself to all the protections of the legalese form
  - "Consumers like it better" vs. "consumers never read privacy statements anyway" battle
- Layered form
  - Relatively simple statement incorporating links to more detailed information
  - Examples Vidyo: http://www.vidyo.com/privacy-policy/ P&G: http://www.pg.com/privacy/english/privacy_notice.shtml

PAI

Content of Privacy Statements

- Content is somewhat dependent on the category of data subjects being addressed
  - A consumer privacy statement will not have the same content as an employee privacy statement, although some elements (e.g. security) may be similar
  - Some specialized privacy statements have mandatory content (to be discussed later)
  - Care must be taken to carefully determine the scope of data subjects being addressed – e.g. are retirees included in the employee statement? Job applicants?
- Let's examine the subjects covered in a typical **consumer** privacy statement

Typical Content of Privacy Statements

- Sources of information covered
  - Online? Which ones?
  - Off line?
- Information Collected
  - From data subject
  - By electronic means unseen to the consumer
  - From third parties
  - Can get very technical – good argument for layered statement
- How Collected Information is Used
  - Commercial uses of each type of information
  - Respond to compulsory process (may be put in third party transfer section)
    - Who decides if process is valid?
    - Opportunity for challenge by data subject?
  - Use to protect entity or others
    - What about informal government requests: “the terrorists are about to explode the bomb, we need this information immediately to save lives”
    - Protecting employees from immediate harm

PAI

Typical Content of Privacy Statements

- Where Collected Information is Stored
- How Long it is Retained
- Use of Cookies/Tracking Mechanisms
- With Whom Collected Information is Shared
  - Affiliated entities?
  - Other third parties?
  - Suppliers
    - Very likely, particularly suppliers in IT area
    - Normal to include statement that supplier is under contractual obligation to use the information only to provide services to the entity – but make certain that is true!

PAI

Typical Content of Privacy Statements

- Information Security Explanation
  - FTC's position is that not having adequate security for consumer information (evaluating actual risks to collected information and addressing those risks based on sensitivity of information) is unfair for Section 5 purposes
  - No matter how extensive the entity's infosec program, leave wiggle room in language
- Available Choices Given to Data Subjects
  - Opt in/opt out of various marketing or data sharing programs (perhaps a link to a preference page)
  - Be sure to keep difference between removal of name and suppression of name in mind while drafting
  - How data subject information can be updated
  - Reference to possible choices by entity's data analytics programs

Typical Content of Privacy Statements

- COPPA Notice
- California “Shine the Light” Notice
  - Applicable to information on California residents entity shared with third parties for marketing purposes over prior calendar year
  - Critical that processes allowing identification and disclosure of this information are in place
- Changes to Privacy Statement – Effective date
- Contact Information for the Entity Publishing the Statement

Specialized Privacy Statements

Examples of Specific Disclosure Requirements

- HIPAA
  - PHI - ePHI
  - “required by law to maintain the privacy of protected health information”
- Safe Harbor/Privacy Shield
  - Required right of access
  - Dispute resolution body/process
- GLBA
  - Customer v Consumer
  - NPI