



PAI

Privacy Associates International, LLC

A Guide to Privacy Law

Robert L. Rothman

3rd Annual Information Technology Law Seminar

September 22, 2010

Introduction

- What is privacy?
- Origins and nature of American privacy law
- Selected major issues
 - General
 - Privacy statements
 - Security issues
- Privacy outside the U.S.
- Hot issues
 - Cloud computing
 - Behavioral tracking

What is privacy?

The Definition of Privacy

- *Privacy is having control over one's personal information*
- That control over information allows us to portray different images of ourselves in our different life roles, depending on the personal information we choose to reveal.

Professional/Attorney

Lover/spouse

Parent

Child

Friend

Foe

Boss

Subordinate

- Control was never absolute and today is less likely to be so
 - Ease of reproduction, transmittal and storage
- Privacy definition must also include an element of *control of access to the self* – who can access me when and how

Personal Information

- If privacy includes the control of personal information, what is personal information?
- Literally hundreds of definitions of the term
- In the US, have to consider the issue under each individual statute
 - Tend to be narrower definitions, e.g. Michigan breach law defines personal information as:

“...the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state: (i) Social security number. (ii) Driver license number or state personal identification card number. (iii) Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.”

- Different terms sometimes used for personal information, eg “Protected Health Information” under HIPAA

Personal Information

- Most other countries have omnibus privacy laws that provide rules for dealing with personal information in whatever context it arises
- For instance, the European Union Data Protection Directive, which has become the model for most of the world outside the US, defines “personal data” as:
 - **“... any information related to an identified or identifiable living natural person”**
 - Very broad definition
 - Also very clear

Origins of U.S. Privacy

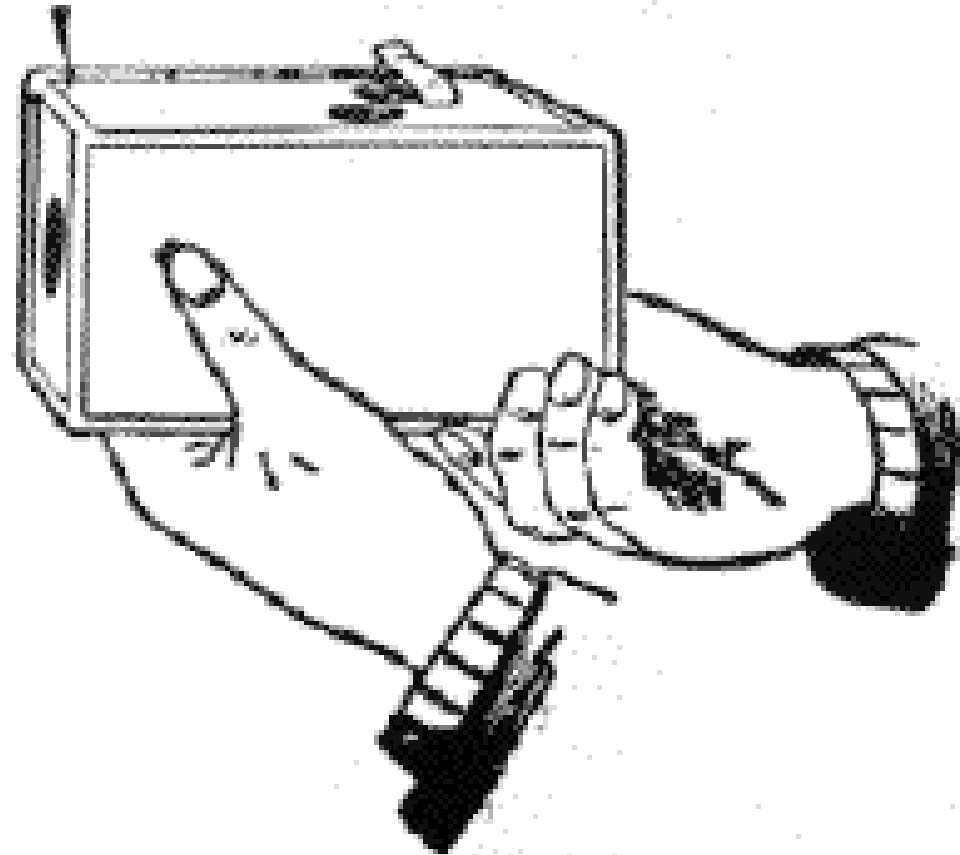
US Constitution

- No explicit privacy right, although a zone of privacy recognized in its “penumbras,” including:
 - 1st amendment (right of association)
 - 3rd amendment (prohibits quartering of soldiers in homes)
 - 4th amendment (prohibits unreasonable search and seizure)
 - 5th amendment (no self-incrimination)
- Rights under some state constitutions

Origins of US Privacy

- Privacy in US originated from tort law
- The tort law was created as a direct result of scary new technology

THE KODAK CAMERA



Price \$25.00.

The Eastman Dry Plate & Film Co.
ROCHESTER, N. Y.

100

**Instantaneous
Pictures!**

Anybody can use it.

No knowledge of
photography is
necessary.

The latest and
best outfit for ama-
teurs.

Send for descrip-
tive circulars.

Origins of US Privacy

- The Warren & Brandeis Article: The Right to Privacy 4 Harv. L. Rev. 193 (1890)
 - Arguably most famous, and certainly most influential, law journal article in US legal history
 - Argued that a right to privacy exists in the in the common law
- Written as reaction to the “yellow press”
 - Gossip and hearsay articles
 - Provided publication to private facts
 - Threatening new technology “instantaneous photography” exacerbated problem

The Right to Privacy

- Authors point to other protections the common law provides for:
 - The right to determine the extent to which our thoughts are communicated to others
 - The protection of letters, diaries, etchings and art
 - The protection of a catalogue of one's etchings
 - The right not to be assaulted or beaten
 - The right not to be imprisoned
 - The right not to be maliciously prosecuted
 - The right not to be defamed
- Authors then assert that all of these rights derive from a more general common law principle: ***the right to be let alone*** a term coined by Michigan's own Thomas M. Cooley in his treatise on the law of torts

Prosser's Torts

- Prosser identified (in 1960s) four distinct torts that developed out of the 1890 Warren & Brandeis article
 - Intrusion upon seclusion
 - Public disclosure of private facts
 - False light
 - Appropriation of name or likeness
- Adopted by the Restatement of Torts
 - Collectively known as Invasion of Privacy

U.S. Federal and State Privacy Laws

Fair Information Practices

U.S. Dept. of Health, Education and Welfare, 1973

- **Collection limitation.** There must be no personal data record keeping systems whose very existence is secret.
- **Disclosure.** There must be a way for an individual to find out what information about him is in a record and how it is used.
- **Secondary usage.** There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- **Record correction.** There must be a way for an individual to correct or amend a record of identifiable information about him.
- **Security.** Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

US Privacy Development

- 1970's – US Privacy Act (applicable to government)
- 1980's - OECD Principles laid foundation for more consistent global privacy legislation
- 1980's & 1990's - Direct marketing, telemarketing and other annoyance issues, healthcare issues, financial privacy
- 2000's – Identity theft and security issues

US Statutory Approach to Privacy

- US now a hodge-podge of hundreds of federal and state privacy laws that deal with privacy in different contexts
- Each statute is aimed at different problem and has different definitions of what constitutes personal information
- Incomprehensible system for those outside the US

Examples of Federal Laws

- **Cable Communications Policy Act**
- **CAN-SPAM Act**
- **Children's Online Privacy Protection Act**
- **Computer Matching and Privacy Protection Act**
- **Consumer Credit Reporting Reform Act**
- **Driver's Privacy Protection Act**
- **Electronic Communications Privacy Act (ECPA)**
- **Electronic Funds Transfer Act**
- **Electronic Signatures in Global and National Commerce Act**
- **Employee Polygraph Protection Act**
- **Fair and Accurate Credit Transaction Act (FACTA)**
- **Fair Credit Reporting Act (FCRA)**
- **Family Educational Rights and Privacy Act**
- **Financial Services Modernization Act (aka Gramm-Leach-Bliley)**
- **Foreign Intelligence Surveillance Act**
- **Freedom of Information Act**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **Identity Theft and Assumption Deterrence Act**
- **Privacy Act of 1974**
- **Privacy Protection Act of 1980**
- **Right to Financial Privacy Act**
- **Telecommunications Act**
- **Telemarketing and Consumer Fraud Act**
- **Video Privacy Protection Act**
- **Video Voyeurism Prevention Act**

Selected Areas of State Legislation

- Identity theft protection
- Security breach notification
- Social security number protection
- Marketing
- Spyware and adware
- Radio frequency identification devices
- Insurance
- Vehicle data event recorders
- Background checks
- Online background checks

Privacy Statement Issues

Privacy Statements

- Statements that explain to consumers what personal information is being collected, the purpose of use, with whom the information is shared, choices available, etc.
- Harken back to the 1973 Fair Information Practices
- Certain laws require these kinds of consumer notifications
- Graham-Leach-Bliley (GLB)
 - requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter
 - The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected, and. also identify the consumer's right to opt out of the information being shared with unaffiliated parties pursuant to the provisions of the Fair Credit Reporting Act
- HIPAA
 - Each covered entity must provide a notice of its privacy practices, including:
 - The ways in which the covered entity may use and disclose protected health information.
 - The covered entity's duties to protect privacy
 - A description of the individuals' rights of redress
 - A point of contact for further information and for making complaints
- California "Shine the Light" Law
 - Must inform customers that they are entitled to request and obtain customer information shared with other businesses for their own direct marketing uses
 - "Your California Privacy Rights" sections of privacy statements

Privacy Statements

- FTC very active in this area “say what you do and do what you say”
 - Recent FTC consent decree arising out of XY Magazine bankruptcy is typical
- Generally the motivation for privacy statements is a perceived competitive need
- Is that the case? Who reads privacy statements? Is notice and choice effective?
- New approaches are being developed

Security Issues

Security Issues

- Security a subset of privacy – to maintain privacy must be able to assure that personal information in the hands of a proper holder is not dispersed to others
- Security is one of the privacy matters of greatest visibility in the US
- Often speak of three elements of information security: physical, technical and administrative
 - Often in different corporate silos – takes a combination of legal, IT and physical security people to determine what law requires
 - Coordination can be a challenge

Security Issues

- Liability sources:
 - FTC Act
 - State security breach notification laws, analogous laws outside the US
 - U.S. Federal laws: FCRA, GLB and FACTA (financial) HIPAA and HITECH (medical), proposed federal data security bills
 - Tort liability
 - Loss of customer trust/reputational risk

Federal Trade Commission

- **Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in commerce.”**
- **FTC very active in using these powers to go after companies that have had personal data breaches.**
- **Early cases focused on “deception” theory: the entity didn’t do what it said it would do**
- **More recent cases have used “unfairness” theory: doesn’t matter what you promise, simply unfair not to provide adequate security to consumer personal information**
- **Extremely difficult to pass on responsibility to suppliers, beyond financial indemnification**

State Data Security Breach Statutes

- While there are many commonalities, there are also many differences
- Breach of a database with consumers from different states requires examination of each state's law to see how personal information is defined
- Even what constitutes a breach and when notification has to be made differ
- Emerging issue: how hard do you have to look for a breach?

State Data Security Breach Statutes

- In California, “personal information” is an individual’s first name or first initial and last name, in combination with any one or more of:
 - (a) SSN; (b) DLN or California ID number; or (c) account number, CCN or DCN in combination with any required security or access code or password that would permit access to an individual’s financial account
- In addition to common California elements, personal information definition may include
 - Mother’s maiden name
 - Date of birth
 - Employer identification
 - Computer password
 - Electronic signature
 - Biometric ID

State Security Breach Laws

- Other State variations
 - Private rights of action
 - Notification to state administrative agencies such as police departments, consumer protection entities or state attorney generals
 - Notification to national credit bureaus if > 500 persons affected
 - “Security breach” includes breaches of encrypted data transferred to unauthorized persons with encryption keys

State Data Security Breach Statutes

- Practical, non-legal aspects of a security breach can be overwhelming to the client, e.g.
 - What exactly was on the stolen laptop? Was it encrypted? When are we sure the mainframe was hacked and personal information exposed?
 - How do we get out 300,000 letters to people whose personal information may have been compromised? How do we tell them
 - Do we offer something to the victims to try to retain goodwill? Credit monitoring? Identity theft insurance?
 - Can we quickly set up a call center to answer questions?
 - Do we have an established internal process for dealing with all this? Who is the decision-maker?

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
 - Make certain that contracts with outside suppliers that handle personal information have appropriate security language, including notification and cooperation provisions
 - Make certain that you have systems and processes to discover or become informed of a breach
 - Make certain that the company has a well thought out process involving the right people to respond quickly and decisively to any personal information security breach that does occur

Privacy Outside the US

Differences Among National Approaches

- Ominibus vs. Sectoral Approach
- Collecting personal information is inherently bad and should be prohibited unless authorized by law vs. collecting personal information is neutral but misusing that information is bad and should be prohibited
- Historical and constitutional antecedents

Where is the Problem?

Countries outside the US with omnibus privacy legislation include:

Belgium	Luxembourg	Argentina	Iceland
Bulgaria	Hungary	Canada	Liechtenstein
Czech Republic	Malta	Mexico	Norway
Denmark	Netherlands	Uruguay	
Estonia	Austria		Switzerland
Germany	Poland	Israel	Russia
Greece	Portugal	UAE (Dubai International Financial Centre)	
Spain	Romania		Australia
France	Slovenia		Japan
Ireland	Slovakia		New Zealand
Italy	Finland		[Hong Kong]
Cyprus	Sweden		
Latvia	United Kingdom		

What do these laws require?

- Each law, even within the EU, is different
- Generally specify the circumstances under which personal information can be collected – often require registration with the data protection authorities
- Generally specify how collected personal information has to be treated
- Most (not all) prohibit the transfer of personal information out of the country to a jurisdiction with inadequate privacy laws unless a legal basis is put in place

Cross-border Transfer of Personal Info

- Cross-border transfer limitations is one reason these laws are significant to US entities
 - US is universally regarded as not having adequate privacy laws
 - To get personal information (not a narrow US definition) to the US, must fall under one of the limited legal exceptions
- Creates significant issues for US business
 - Company operations
 - Having personal information processed in these countries
 - SOX whistleblower issues
 - US discovery, particularly e-discovery compliance
 - US security arrangements – airline passenger lists

Current Hot Privacy Issues

Cloud Computing

- Software as a service, infrastructure as a service, etc
- Public clouds and private clouds
- Governance risks
 - Retaining rights to personal information vis-à-vis supplier
 - Allows for switching suppliers and maintains better bargaining power dynamics
- Compliance risks
 - Often cannot reallocate these risks – e.g. security - from the standpoint of responsibility
 - Can provide for financial indemnification
- Many privacy legal concepts do not readily fit into the cloud computing model

Behavioral Tracking

- If your online behavior – what you look at, how long, etc. – is tracked and recorded and used to serve you ads and make you commercial offers, but never linked to your name, is there a privacy problem?
- FTC has been reviewing and holding information gathering sessions for years now and at one point proposed some fairly onerous rules
- In Europe informed consent required

Conclusion

- Privacy issues here to stay – there are few lawyers, regardless of area of practice, who will not have to know about at least some aspects of the subject
- Technology and privacy have been linked from the beginning and will undoubtedly continue to be linked
- IT lawyers have a particular need to be familiar with global privacy laws