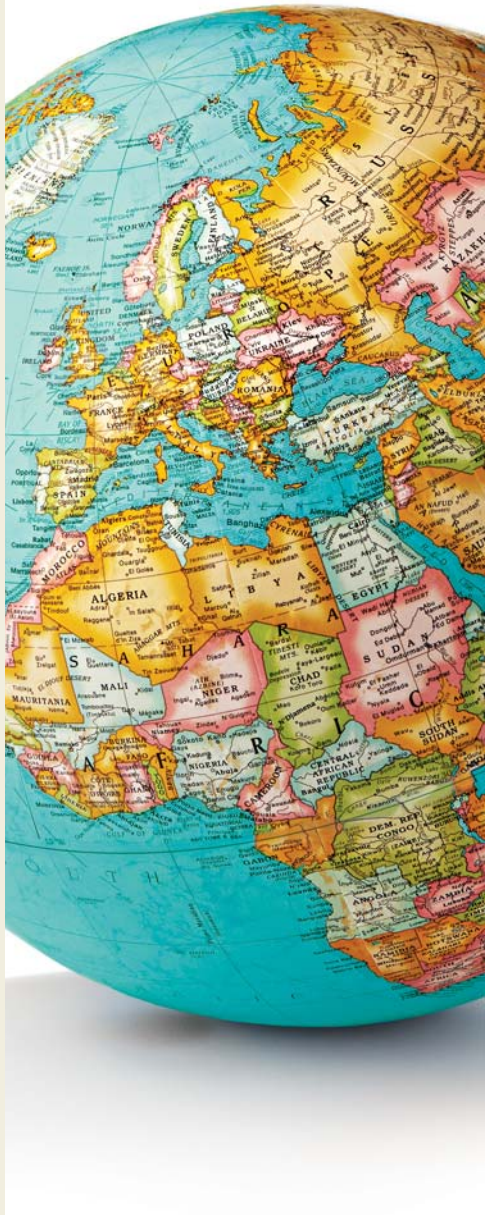
SQUIRE SANDERS

U.S. Information Privacy Law

Ivan Rothman
Joseph Grasser

January 28, 2014



SQUIRE SANDERS

Introduction and Agenda

- Sources of US Privacy Law
- Some Basic Concepts
- Sectors of US Privacy Law
- Non-Sector Specific Issues
  - Privacy Notices
  - Information Security
  - Compliance with Breach Notification Statutes
- EU and Safe Harbor Principles
- Practical Conclusions

SQUIRE SANDERS

Sources of US Privacy Law

- Sources of US privacy law are as varied as US law itself and include:
  - US and state constitutions;
    - Fourth Amendment
    - Supreme Court
  - federal and state legislation;
    - Prosser's four privacy torts
  - regulations promulgated by government agencies and related consent decrees;
    - FTC
  - federal and state case law and common law principles, in particular contract and tort law; and
  - contracts and even privacy policies can give rise to enforceable rights and obligations re: privacy matters.

SQUIRE SANDERS

Some Basic Concepts

- Privacy
- Information Privacy
- Personal Information (PI)
- Personally Identifiable Information (PII)
- Information Technology
- Identity Theft
  - The Identity Theft Assumption and Deterrence Act (1998)
- Data Protection Law

SQUIRE SANDERS

Some Basic Concepts (con't)

- Information Security Program
  - Administrative safeguards (e.g., written policies, training)
  - Technical safeguards (e.g., encryption, firewalls)
  - Physical safeguards (e.g., locks, security cameras)
- Integrity and Availability
- Privacy Officer
- Choice: opt out versus opt in
- Omnibus versus Sectoral Laws
  - Omnibus: comprehensive approach to protecting PI (common in EU) based on single omnibus law that cuts across different industries and may also regulate both private and public sectors.
  - Sectoral: regulation of PI on sector by sector basis with different industries governed by multiple, different laws.

SQUIRE SANDERS

Basic Sectors of US Privacy Law

- Financial Privacy;
  - 1999 Gramm-Leach Bliley Act (GLBA)
- Medical Privacy;
  - 1996 Health Insurance Portability and Accountability Act (HIPAA)
- School Privacy;
- Children's Privacy;
  - 1998 Children's Online Privacy Protection Act (COPPA)
- Telecommunications Privacy;
- National Security and Public Privacy;
- Workplace Privacy;
- Civil Litigation and Privacy; and
- Media and Privacy

SQUIRE SANDERS

HIPAA

- The basic framework for protecting the privacy and security of certain health-related information ("protected health information" or PHI) – applies primarily to healthcare providers and health plans and insurers. Protects PHI through the Privacy Rule and the Security Rule.

- Basic requirements include:

  - provision to individuals of detailed privacy notice;
  - opt-in authorization for use of PHI for purposes other than treatment, payments and operations;
  - right of individuals to access and copy their PHI;
  - implementation of administrative, technical and physical safeguards to protect the confidentiality and integrity of all PHI; and
  - Designation of a privacy official who is responsible for the development and implementation of privacy.

SQUIRE SANDERS

HIPAA (Con't)

- Creates obligations for "Business Associates" - i.e. third-party entities that performs services or activities on behalf of a covered entity that involve the use or disclosure of PHI, such as claims processing, data analysis and data aggregation.
  - In the past, focus was on required use of "Business Associate Agreement" between covered entity and Business Associate under which Business Associate agreed to comply with certain required privacy and security standards.
  - Now under recent amendments HIPAA privacy and security rules apply directly to business associates – not just contractual liability.
- There are a number of exceptions, including for certain financial transaction services and other services where PHI is not actually being used and access is incidental.

SQUIRE SANDERS

COPPA

- Regulates collection and use of children's PI by operators of commercial websites and online services directed to children under the age of 13, and if operator has actual knowledge that it is collecting PI from such children.
- In determining if website or service is directed to children, FTC considers numerous factors, such as subject matter, visual and audio content, age of models.
- Basic requirements include:
  - Posting of privacy notice on website describing what information is collected from children, how the operator uses such information and the operator's disclosure practices for such information;
  - Obtaining verifiable parental consent for the collection, use or disclosure of PI from children before collecting PI – i.e., opt-in approach.
  - Providing parental access to PI to review or have deleted;
  - Maintaining the confidentiality, security and integrity of PI.

SQUIRE SANDERS

COPPA (Con't)

- Recent amendments include:
  - expanded list of "PI" that cannot be collected without parental consent to include: photographs, videos, geolocation information and persistent identifiers that can recognize users over time and across different websites or online services, such as IP addresses and mobile device IDs;
  - closed a loophole that allowed kid-directed websites and services to permit third parties to collect PI through plug-ins without parental consent; COPPA requirements apply to kid-directed services and third parties);
  - expanded definition of "collect" to include "passive tracking of a child online;" and
  - streamlined processes for new ways of getting parental consent.

SQUIRE SANDERS

Non-Sectoral Specific Issues

The following areas are of general importance to any company that collects PI from customers and consumers even if their activity does not fall within the ambit of specific sectoral laws:

- Privacy Notices
- Information Security
- Compliance with data breach notification statutes

SQUIRE SANDERS

Privacy Notices

- In the mid to late 1990's, companies – despite absence of legal requirement - began to post privacy notices on their websites intended to inform consumers about how their PI was being collected and used. This was done primarily for public relations and reputational reasons.
  - Courts have generally taken the position that privacy notices are not contracts.
  - However, the FTC took the position that failure to act in accordance with promises in the notice re privacy and security constituted a deceptive and /or unfair practice under Section 5 of the FTC Act, regardless of whether the notice would be considered an enforceable contract under contract law principles.

SQUIRE SANDERS

Privacy Notices (Con't)

- FTC Enforcement Actions: grounds for deceptive trade practices complaints
  - Inadequate security
  - Sharing of PII
  - Failure to provide reasonable security to protect PII

  - Recent FTC Actions against Sears, Facebook and Google
    - Sears Case from 2009
      - Consumers paid $10 to download research software and were told it would track their "online browsing" but it actually tracked much more
      - While it was disclosed, it was only disclosed in a lengthy user agreement, that the user did not see until the end of the process
    - Facebook Case
      - Similar to Sears in that true choice
      - Issue was that Facebook was constantly changing the rules
      - The order requires "affirmative express consent" before it can override their own privacy settings
    - Google Case
      - Google was found to be tracking Apple Safari users using cookies when it promised not to track
      - Google, by all appearances, did not intentionally collect the data
      - Made about $4m in profit on the tracking but had to pay a $22.5m in fines (and 20 years of monitoring)

SQUIRE SANDERS

Privacy Notices (con't)

- California Online Privacy Protection Act (2003) requires operators of commercial websites and online services -- located anywhere -- that collect PII from consumers residing in CA to conspicuously post a privacy policy on their website.
  - Since 2012 applies to mobile app developers who collect PII through their apps and services.
  - Does not apply to 3rd parties that operate, host or manage websites or online services on behalf of the first party, such as ISPs.
  - "PII" – information collected about consumers, including name, address, email address, telephone number, SSN and any other similar identifying information.
  - "conspicuously" – the privacy policy is (i) on the homepage of the website, or the first significant page after entering the site; or (ii) hyperlinked to the homepage by an icon or text link that contains the word "privacy" in a color different from the background color.

SQUIRE SANDERS

Privacy Notice (Con't)

- The privacy notice must:
  - identify the categories of PII the operator collects;
  - identify the categories of 3rd parties with whom PII may be shared;
  - describe the process by which consumers may review and request changes to their PII, if such a process exists;
  - describe the process by which the operator notifies consumers of material changes made to the privacy policy described in the notice; and
  - identify its effective date.

SQUIRE SANDERS

Privacy Notices (con't)

- CalOPPA was recently amended to require the privacy notice to disclose:
  - whether other parties (e.g., third-party advertising networks and analytics providers) may collect PII about an individual consumer's online activities over time and across different websites when a consumer uses the operator's website or service; and
  - how the operator responds to Web browser Do-Not-Track signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services, if the operator engages in that collection.
- After receiving notice of noncompliance, the website or online service operator has 30 days to post an appropriate notice and adhere to the terms of the notice. Law is enforced through CA's general consumer protection law that prohibits unlawful, unfair or fraudulent business acts and practices. Actions may be brought by state government officials or private parties.

SQUIRE SANDERS

Information Security

- No comprehensive or omnibus information security law imposing security standards across different industries.
- Many sectoral laws have security-related provisions but often couched in general language.
- Some states have enacted general information security laws.

SQUIRE SANDERS

Information Security (Con't)

- California Data Security Breach Statute (2004): requires a business "that owns or licenses personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the 'personal information' from unauthorized access, destruction, use, modification or disclosure."

  - Provides no guidance as to what constitutes **"reasonable security procedures and practices**."

  - Advisable to adopt financial and healthcare sector frameworks as models and develop a comprehensive written information security program that appropriately responds to the company's size and complexity, the nature and scope of its activities and the sensitivity of the PI that it handles., and to designate an employee or employees to coordinate the company's information security program.

SQUIRE SANDERS

Information Security (Con't)

- The Massachusetts law (Standards for the Protection of Personal Information of Residents of the Commonwealth):
- Establishes detailed minimum standards to "safeguard…personal information … contained in both paper and electronic records," and requires businesses holding such information to:
  - Designate an individual who is responsible for information security;
  - Anticipate risks to PI and take appropriate steps to mitigate such risks;
  - Develop security program rules;
  - Impose penalties for violations of the program rules;
  - Prevent access to PI by former employees;
  - Contractually obligate third-party service providers to maintain similar procedures;
  - Restrict physical access to records containing PI;
  - Monitor the effectiveness of the security program;
  - Review the program at least once a year, and whenever business changes could impact security; and
  - Document responses to incidents.

SQUIRE SANDERS

Information Security (Con't)

- Also mandates certain technical requirements, including user authentication, access controls, monitoring, portable devices, firewall protection, updates and training, as well as encryption "**of all transmitted records and files containing personal information that will travel across public networks … of all data containing personal information to be transmitted wirelessly [and] … of all personal information stored on laptops or other portable devices**."

- Given that compliance with this law is both required if you are collecting and storing PI of Massachusetts residents, and will generally meet the requirements of any other such state laws, it is generally considered advisable to comply with the administrative and technical requirements of the law.

SQUIRE SANDERS

Information Security (Con't)

- The International Organization for Standardization (ISO) is a nongovernmental organization that promulgates and publishes business standards to promote quality across the globe. ISO has two main information security standards:
  - ISO 27001 applies to information security management – provides comprehensive set of controls for information security management; and
  - ISO 27002 outlines international best practices for information security techniques.

SQUIRE SANDERS

Information Security (Con't)

- A security breach is neither a necessary nor a sufficient condition for potential liability: requirements in sectoral and state security laws may be violated in the absence of a breach; there is no strict liability when a breach occurs.
- Deficient security may expose a company to legal action by federal government agencies under sectoral laws, by state AG's under state laws, by the FTC under the fairness standard in Section 5 of the FTC Act and by private citizens under a variety of legal theories.
- Recent cases of note in the latter context are:
  - Sony
    - Still going and key ruling just made
    - Plaintiffs had standing because they alleged plausibly alleged a "credible threat" of impending harm & because they would not have purchased the consoles without promises of security that were not met
    - Most of the claims were still dismissed, but the above holding on damages are likely to have lasting impact
  - Target
    - Huge data breach at retail locations
    - Interesting causes of action include: common law invasion of privacy, bailment and negligence

SQUIRE SANDERS

Data Breach Notification Laws

- Data Breach Notification Laws
  - Incentivize companies to implement effective security controls
  - California Data Breach Notification Law SB-1386
    - Applicable to any person, business or government agency that conducts business in California and that owns or licenses computerized data that include personal information
    - Definition of personal information
    - Disclosure requirements
    - Exceptions

SQUIRE SANDERS

Data Breach Notification Laws (con't)

- Incident management
  - Move expeditiously
  - Assemble incident response team
  - Conduct risk assessment to determine if a breach has indeed occurred and scope of breach and harm to individuals
  - Identify and preserve compromised data
  - Containment and analysis of the incident
  - Determine what notification is required
  - If the incident has created a risk of identity theft, consider notifying affected individuals even if such notification is not required
  - Assess appropriate mitigation measures
  - Develop script for communication with breach subjects
  - Determine what corrective action measures are needed
  - Document all response activity
  - Perform post-notification review of events

SQUIRE SANDERS

EU & Safe Harbor Principles

- EU Data Protection Directive (1995):
  - requires a high level of privacy protection for personal data within all Member States; and
  - permits a transfer of such data to a non-EU Member State only if its laws afford “an adequate level of protection.”
- In 1999 the EU determined that the “current patchwork of narrowly focused sectoral laws … in the U.S. is not adequate.”
- Consequently, U.S. Department of Commerce and EU Commission negotiated a Safe Harbor certification arrangement for personal data transferred from EU to U.S.

SQUIRE SANDERS

EU and Safe Harbor Principles (Con't)

- US companies (excluding financial institutions) that wish to participate must, among other steps, agree to comply with the following seven principles:
  - Notice: notify individuals about the purposes for which they collect and use information about them.
  - Choice: provide opt out and opt in options re disclosure to third parties. Opt in for sensitive information.
  - Onward Transfer: third party must apply notice and choice principles.
  - Access: reasonable access to stored information and ability to amend.
  - Security: "reasonable precautions" to safeguard information.
  - Data integrity: relevant and reliable for intended use.
  - Enforcement: readily available and affordable independent recourse mechanisms for addressing complaints and disputes.
- US companies must annually certify their compliance with US Department of Commerce.
- FTC enforces violations: failure to comply with a promise to abide with the principles is considered a deceptive and unfair trade practice.

SQUIRE SANDERS

Practical Conclusions

- If your organization does not collect PII focus on workplace privacy and protecting proprietary confidential information of company and possibly of actual and potential business partners.

- If your organization collects PII, determine if you fall within the scope of any sectoral laws; if so, ensure you or others within the organization (or outside counsel) have in-depth knowledge of these laws and that the organization complies with them.

- If your organization collects PII but does not fall within the scope of any sectoral laws, you still need to:

SQUIRE SANDERS

Practical Conclusions (Con't)

- Ensure the organization has a robust security system in place and is generally complying with best information security practices.
- Adopt internal privacy policies and practices, post a privacy notice that accurately reflects these policies and practices and comply with them.
- Anticipate and prepare for security breaches and have a plan in place to quickly comply with applicable data breach notification laws.
- Consider encryption of PII – may be required under information security laws and also enable you to avoid having to comply with most data breach notification laws.
- Do not forget compliance with laws re data destruction.

- If your organization collects personal information of EU residents consider obtaining safe harbor certification or adopting modal contractual clauses.

SQUIRE SANDERS

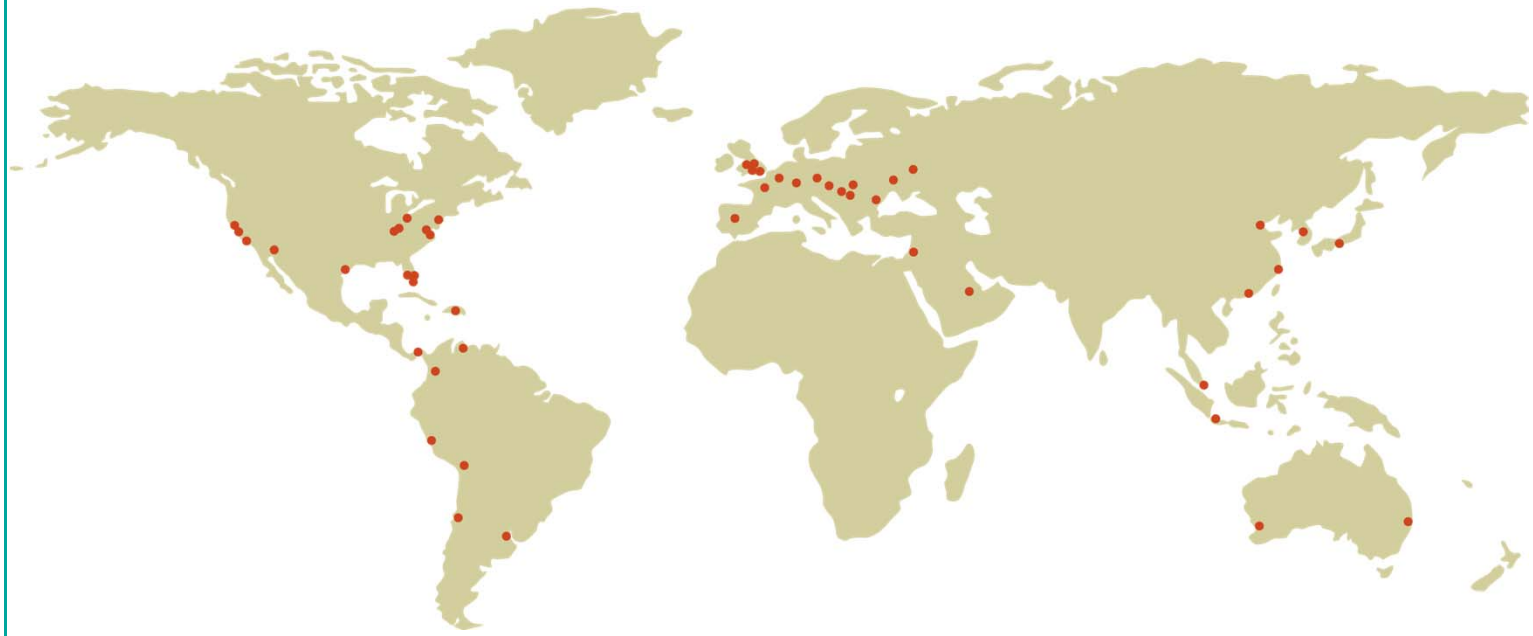
Contact Information

Joseph P. Grasser
joseph.grasser@squiresanders.com
+1 650 843 3386

Ivan Rothman
ivan.rothman@squiresanders.com
+1 415 954 0241

SQUIRE SANDERS

Worldwide Locations



North America

- Cincinnati
- Cleveland
- Columbus
- Houston
- Los Angeles
- Miami
- New York
- Northern Virginia
- Palo Alto
- Phoenix
- San Francisco
- Tampa
- Washington DC
- West Palm Beach

Latin America

- Bogotá+
- Buenos Aires+
- Caracas+
- La Paz+
- Lima+
- Panamá+
- Santiago+
- Santo Domingo

Europe & Middle East

- Beirut+
- Berlin
- Birmingham
- Bratislava
- Brussels
- Bucharest+
- Budapest
- Frankfurt
- Kyiv
- Leeds
- London
- Madrid
- Manchester
- Moscow
- Paris
- Prague
- Riyadh
- Warsaw

Asia Pacific

- Beijing
- Hong Kong
- Jakarta+
- Perth
- Seoul
- Shanghai
- Singapore
- Sydney
- Tokyo

+ Independent Network Firm