Rossdale CLE

Data Privacy Laws in the United States

Mastering Internet, Social Media, & Privacy Law

Live Telephonic Seminar on April 30, 2014

www.RossdaleCLE.com

Data privacy laws in the United States

There is no single, comprehensive federal law regulating the collection and use of personal data.

The US has a **patchwork** system of federal and state laws.

In addition, there are many governmental agency regulations.

This patchwork system is slated to change due to the numerous security breaches which occur on an almost daily basis.

What follows is a partial list of some laws related to data collection

Two Types of Information

- Personally identifiable information” (PII) can be linked to a specific individual
  - Name, e-mail, full postal address, birth date, Social Security number, driver’s license number, account numbers
- “Non-personally identifiable information” (non-PII) cannot, by itself, be used to identify a specific individual

Laws that Protect PI

- Data privacy laws govern businesses' collection, use, and sharing of information about individuals
- Federal, state, and foreign laws apply
- Laws govern both physical and electronic security of information

The “Gray Area”-- PII or Non-PII?

- Anomyzed” data that is “de-anomyzed”
  - IP address linked to domain name that identifies a person

- Non-PII that, when linked with other data, can effectively identify a person – “persistent identifiers”
  - Geolocation data
  - Site history and viewing patterns

U.S. Laws Are A Patchwork

Americans with Disabilities Act (ADA) - Primer for business.
Cable Communications Policy Act of 1984 (Cable Act)
California Senate Bill 1386 (SB 1386) - Chaptered version.
Children's Internet Protection Act of 2001 (CIPA)
Children's Online Privacy Protection Act of 1998 (COPPA)
Communications Assistance for Law Enforcement Act of 1994 (CALEA) - Official CALEA website.
Computer Fraud and Abuse Act of 1986 (CFAA) law summary. Full text at Cornell
Computer Security Act of 1987 - (Superseded by the Federal Information Security Management Act (FISMA)
Consumer Credit Reporting Reform Act of 1996 (CCRRA) - Modifies the Fair Credit Reporting Act (FCRA).

Patchwork (cont.)

- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003
- Electronic Funds Transfer Act (EFTA) Summary
- Fair and Accurate Credit Transactions Act (FACTA) of 2003
- Fair Credit Reporting Act (Full Text).
- Federal Information Security Management Act (FISMA)
- Federal Trade Commission Act (FTCA)

Patchwork (cont.)

- Driver's Privacy Protection Act of 1994 .
- Electronic Communications Privacy Act of 1986 (ECPA)
- Electronic Freedom of Information Act of 1996 (E-FOIA) Discussion as it related to the Freedom of Information Act.
- Fair Credit Reporting Act of 1999 (FCRA)
- Family Education Rights and Privacy Act of 1974 (FERPA; also know as the Buckley Amendment)
- Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)
- Privacy Act of 1974 - including U.S. Department of Justice Overview
- Privacy Protection Act of 1980 (PPA) - Additional discussion at http://www.epic.org/privacy/ppa/.
- Right to Financial Privacy Act of 1978 (RFPA)

Patchwork (cont.)

- Telecommunications Act of 1996
- Telephone Consumer Protection Act of 1991 (TCPA) - Text of law at http://www.law.cornell.edu/uscode/47/227.html
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
- Video Privacy Protection Act of 1988

FTC

- The FTC continues to be an active enforcer of privacy and data security laws and regulations. In 2012, the federal agency:
- •Charged the operator of a website and mobile app with collecting personal information from a users' mobile device contacts lists without users' knowledge or consent.
- •Settled charges with a mobile device manufacturer over allegations that it failed to take reasonable steps to secure personal information on its smartphones and tablets.
- •Charged an online market research company with violating its own privacy policy by collecting personal information such as usernames and passwords, financial account numbers, social security numbers, and credit card numbers.
- •Settled charges with a payday lender that improperly disposed of customers' financial information in unsecured dumpsters near its stores.
- •Levied a fine of US$1 million against the operator of music recording stars' fan websites for collecting personal information from children under 13 without parental consent.

FTC

- The FTC also issued best practices for companies that utilise facial recognition technology and, in March 2012, the FTC issued its long-awaited report called Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers which proposes a new privacy "framework" for protecting consumer privacy and calls on industry to improve self-regulatory efforts. The FTC's report followed the Obama Administration's Consumer Privacy Bill of Rights which provides a modern expansion of the traditional Fair Information Practice Principles (FIPPs) and seeks to bring America more in step with how Europe, Canada and other jurisdictions with more mature privacy frameworks protect their citizens' rights to privacy, while preserving flexibility for businesses in how to most effectively implement them.

The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act)

- Prohibits "unfair or deceptive practices in or affecting commerce." No need to prove intent.
  - A practice is "unfair" if:
    - It causes or is likely to cause substantial injury to consumers
    - It cannot reasonably be avoided by consumers
    - It is not outweighed by countervailing benefits to consumers or to competition
  - A representation, omission, or practice is "deceptive" if:
    - It misleads, or is likely to mislead, consumers
    - Consumers' interpretation of it is reasonable under circumstances
    - It is material

FTC

- Practices attacked by FTC as “deceptive”:
  - Violating published privacy policies
  - Downloading spyware, adware onto unsuspecting users’ computers
  - Failing to verify identity of persons to whom confidential consumer information was disclosed
- Practices attacked by FTC as “unfair”:
  - Failing to implement reasonable safeguards to protect privacy of consumer information

CAN-SPAM Act

- Controlling the Assault of Non-Solicited Pornography and Marketing
- Prohibits fraudulent, abusive, deceptive commercial email
- “One-bite” rule:
  - Business may send unsolicited commercial email message, properly labeled, to consumer, with easy means for consumer to opt out. If the consumer opts out, business may no longer send emails

CAN-SPAM Act

- Commercial email broadly defined as having primary purpose to advertise or promote commercial product or service
- Does not apply to transactional emails, which facilitate or give update on agreed-upon transaction
- Business must monitor third party handling email marketing to ensure compliance
- Pre-empts state statutes, but states may enforce sections of Act addressing fraudulent or deceptive acts, computer crimes, other advertising restrictions

Children's Online Privacy Protection Act

- Applies to operators of commercial websites and online services that collect information from children under age 13
  - "No one knows you're a dog on the internet."
- Requires reasonable efforts to get verifiable consent of parent or guardian or to notify parent or guardian
- Requires notice of
  - What information is collected from children
  - How information is used
  - How information is shared

Children's Online Privacy Protection Act

- Prohibits conditioning child's participation in an activity on disclosure of more PI than is necessary
- Amendments effective July 1, 2013
  - Include geo-location information, photos, and videos in types of PI that cannot be collected without parental notice and consent
  - Provide streamlined approval process for new ways to get parental consent
  - Require website operators to take reasonable steps to release children's PI only to companies capable of keeping it secure

Telephone Consumer Protection Act

- Established national “Do Not Call” registry
- Regulates use of “automated telephone equipment” such as auto-dialers, artificial or pre-recorded voice messages, fax machines
- Prohibits transmission of a “call” using an “automatic telephone dialing system” without prior consent of called party
- Per FCC, “call” covers both voice calls and text messages (even texts for which called party is not charged)

Telephone Consumer Protection Act

- Enforcement by federal or state authorities
- Individuals may bring civil actions
  - Papa John's class action over text messages claimed violations of TCPA, Washington Consumer Protection Act
- Relief can include injunction, actual damages, statutory damages of $500 per violation, treble damages

HIPPA

- The federal Department of Health and Human Services (HHS) announced the first settlement involving failure to comply with federal medical breach notification rules (pursuant to the Health Insurance Portability and Accountability Act or HIPAA), and the payment of a US$1.5 million fine by a health insurance company for alleged violations of HIPAA privacy and security rules. HHS also issued its new “Omnibus Rule”, which revises the HIPAA Privacy, Security, Breach Notification and Enforcement Rules. The Omnibus Rule is effective from 26 March 2013, and compliance is required with respect to most provisions no later than September 23, 2013.

HIPAA

- The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. HIPAA is also known as the Kennedy-Kassebaum Health Insurance Portability and Accountability Act (HIPAA-Public Law 104-191), effective August 21, 1996. The basic idea of HIPAA is that an individual who is a subject of individually identifiable health information should have:
- Established procedures for the exercise of individual health information privacy rights.
- The use and disclosure of individual health information should be authorized or required.

HIPAA

- One difficulty with HIPAA is that there must be a mechanism to authenticate the patient who demands access to his/her data. As a result, medical facilities have begun to ask for Social Security Numbers from patients, thus arguably decreasing privacy by simplifying the act of correlating health records with other records. The issue of consent is problematic under HIPAA, because the medical providers simply make care contingent upon agreeing to the privacy standards in practice.

Fair Credit Reporting Act

- The Fair Credit Reporting Act applies the principles of the Code of Fair Information Practice to credit reporting agencies. The FCRA allows individuals to opt out of unwanted credit offers:
- Equifax (888) 567-8688 Equifax Options, P.O. Box 740123 Atlanta GA 30374-0123.
- Experian (800) 353-0809 or (888) 5OPTOUT P.O. Box 919, Allen, TX 75013
- Trans Union (800) 680-7293 or (888) 5OPTOUT P.O Box 97328, Jackson, MS 39238.
- Because of the Fair and Accurate Credit Transactions Act, each person can obtain a free annual credit report.

FCRA

- The Fair Credit Reporting Act has been effective in preventing the proliferation of specious so-called private credit guides. Previously, private credit guides offered detailed, if unreliable, information on easily identifiable individuals. Before the Fair Credit Reporting Act salacious unsubstantiated material could be included, in fact gossip was widely included in credit reports. EPIC has a FCRA page. The Consumer Data Industry Association, which represents the consumer reporting industry, also has a Web site with FCRA information.

FCRA

- The Fair Credit Reporting Act provides consumers the ability to view, correct, contest, and limit the uses of credit reports. The FCRA also protects the credit agency from the charge of negligent release in the case of misrepresentation by the requester. Credit agencies must ask the requester the purpose of a requested information release, but need make no effort to verify the truth of the requester's assertions. In fact, the courts have ruled that, "The Act clearly does not provide a remedy for an illicit or abusive use of information about consumers" (Henry v Forbes, 1976). It is widely believed that in order to avoid the FCRA, ChoicePoint was created by Equifax at which time the parent company copied all its records to its newly created subsidiary. ChoicePoint is not a credit reporting agency, and thus FCRA does not apply.

Fair Debt Collection Practices Act

- The Fair Debt Collection Practices Act , like the FCRA limits dissemination of information about a consumer's financial transactions. It prevents creditors or their agents from disclosing the fact that an individual is in debt to a third party, although it allows creditors and their agents to attempt to obtain information about a debtor's location. It limits the actions of those seeking payment of a debt. For example, debt collection agencies are prohibited from harassment or contacting individuals at work. The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (which actually gutted consumer protections, for example in case of bankruptcy resulting from medical cost) limited some of these controls on debtors.