Davis Wright Tremaine LLP

Anchorage | Bellevue | Los Angeles | New York | Portland | San Francisco | Seattle | Shanghai | Washington, D.C.

Data Protection in the United States

Bruce E. H. Johnson
Chair, Privacy and Security Group
Davis Wright Tremaine LLP

Pacific Rim Advisory Council
Singapore, October 18, 2011

Overview of US Privacy Regulations

- Sector-specific regulations still very strong and growing (both state and federal)
- Transaction-oriented privacy protections, involving commercial use of consumer data
- Class action litigation, with plaintiffs' lawyers seeking development of comprehensive federal privacy liability, is still generally unsuccessful
- Increasing likelihood of federal regulation, more state regulations (how to coordinate with EU model)
- US Supreme Court's June 2011 decision on First Amendment rights in data (*Sorrell*)

Basic Structure of US Data Privacy Regulations

- Sector-by-sector regulations, especially at federal level
- Traditional target is government privacy breaches
  - US Constitution 4th Amendment (1791) prohibits "unreasonable searches and seizures"
    - What is "reasonable expectation of privacy"?
    - Privacy and technology cases since *Olmstead v. United States* (1928) (bootlegger gets wiretapped, holding reversed in 1967)
    - *United States v. Jones* (involving GPS monitor planted on car, will be argued in the US Supreme Court on Nov. 8, 2011)
      - DC Circuit stated: "A person who knows all of another's travels can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts."
  - State Constitutions have similar prohibitions
    - California provision (1972) is the broadest, and gives each citizen "inalienable right" to pursue and obtain "privacy"
    - Also, US 1st Amendment provides a right to anonymous communications (*McIntyre*, 1995)

Basic Structure of US Data Privacy Regulations

- Historically, these have been state regulations
  - Common law
    - Brandeis and Warren tort theories (*The Right to Privacy*, 1890)
    - Includes other confidentiality duties (*e.g.*, privilege rules)
  - State statutes
    - Privacy regulations are usually ad hoc enactments
    - California Office of Privacy Protection lists examples
      - Is a comprehensive data protection regime evolving at the state level (at least in some US states)?
      - The newest California privacy law is the Reader Privacy Act of 2011, effective Jan. 1, 2012, which will require government agencies to obtain a court order before they access customer records from book stores or online retailers.

Examples of Federal Sector-By-Sector Privacy Regulations

- Health (HIPAA, Hi-TECH, etc.)
- Financial (GLBA, FCRA, FACTA, etc.)
- Federal employee and personal records (Federal Privacy Act)
- Drivers' license records (DPPA)
- Video rentals (VPPA)
- Educational records (FERPA)
- Children's online activities (COPPA)
- Computer storage and transmission (ECPA from 1986, includes SCA, CFAA)
- NOTE: law enforcement exceptions

Current Federal Privacy Regulators

- FTC Act prohibits unfair and deceptive acts and practices in commerce
  - Proposed fair information practices (guidelines)
  - Also, generally, enforces privacy principles through consent judgments
  - For example, *Eli Lilly* (Jan. 2002, disclosure of Prozac users' email addresses), *Petco* (Nov. 2004, violation of website's privacy promises), *B.J.'s Wholesale* (June 2005, failure to safeguard customer data), and *Google* (March 2011, failure to inform Gmail users of disclosure of consumer data with Buzz).
  - "Although Google led Gmail users to believe that they could choose whether or not they wanted to join the network, the options for declining or leaving the social network were ineffective. For users who joined the Buzz network, the controls for limiting the sharing of their personal information were confusing and difficult to find, the agency alleged."
- FCC regulates telecoms, etc.
- DOC negotiated "safe harbor" procedures with EU and Switzerland
- Other agencies, also state regulators (usually, the state's attorney general) may become involved, with possible private litigation as well

Federal Restrictions on Marketing Techniques

- Do-Not-Call (also similar state laws) – FTC has Telemarketing Sales Rule ("TSR") and FCC has Telephone Consumer Protection Act ("TCPA") rules – very popular among Americans
  - Junk Fax Law (also state laws) – enforced by private litigants
  - Robocalls and ADADs (also state laws)
- CAN-SPAM (also similar state laws)
  - Recent FTC case (*Flora*) involving unsolicited text messages
    - FTC, on Sept. 29, 2011, stated that Flora "sent a 'mind-boggling' number of unsolicited commercial text messages pitching mortgage modification services to consumers, and misrepresented that he was affiliated with a government agency"
    - Flora's text messages also went to numbers on National Do-Not-Call Registry
    - No opt-out mechanism
    - Also subject to FCC jurisdiction
- Differences with EU (cookies, for example – are they opt-in or opt-out?)
  - What about "super-cookies"?

State Developments: Data Breach Laws

- Data breach notice laws
  - First enacted in California in 2004, now in 46 states, plus DC
  - Even customers' postal codes are "personal information" (*Pineda*, 2011)
  - Laws are not uniform; generally cover state's residents, except Texas, where HB 300 (2011) claims extra-territorial application
  - EU is adopting data breach notice requirements
  - Federal legislation is also very possible, with several bills pending in the US Congress (major dispute is over scope of preemption)

Encryption and PII

- Mass. Gen. L. ch. 93H; 201 CMR 17.00 (broad-reaching Massachusetts data privacy law applies to all companies, wherever located, that use personal data of MA residents; companies must encrypt personal information of MA residents, including data stored on laptops and other portable devices such as BlackBerrys).

- Other states also have laws requiring encryption of personal information. For example, businesses in Nevada must encrypt "customers'" personal information that is transmitted over the internet to recipients outside of the businesses' secure systems (Nev. Rev. Stat. § 597.970).

- Identity Theft Laws and "PII" – *In re Borders Group* (Sept. 27, 2011) (Barnes & Noble must get consumer consent).

Current Issues in US Privacy Regulation

- Increasing federalization of US privacy law
  - FTC decisions – impose greater duty than mere compliance with privacy policies (unfair or deceptive?)
  - FTC and DOC issued privacy reports in 2011
  - Several privacy bills (including private breach notification bills) pending in Congress
  - MIT Prof. Catherine Tucker at Congressional hearing on Sept. 15, 2011, stated that EU opt-in system would cost US companies $33 billion over five years: "There are risks to consumers if companies have unfettered access to consumers' data, but there is also a risk that strict regulations could damage the ability of internet firms to support free services through advertising."
- Behavioral marketing techniques – will they be regulated and how?
  - 2010 – FTC proposed "do-not-track" legislation

Harmonization with EU Data Protection Principles

- FTC and DOC proposals (follow EU model, except for opt-out)
- Safe Harbor (must be subject to FTC or DoT regulation)
  - Advantages include: Simplicity (annual self-certification to DOC)
  - Also, all 27 Member States of EU will be bound by the Commission's finding of adequacy
  - Organizations participating in the U.S.-EU Safe Harbor program will be deemed adequate and data flows to those organizations will continue
  - Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted
- Claims brought by EU citizens against US organizations will be heard in US, subject to limited exceptions

US Constitutional Concerns

- US Constitutional concerns, especially First Amendment, which prohibits laws abridging free speech, will play a role in the ultimate scope of US privacy regulations

- In June 2011, *Sorrell* struck down Vermont privacy law restricting marketing to doctors based on their past history of writing drug prescriptions:
  - Statute aimed at deterring name-brand drug marketing, making it less effective
  - Justice Kennedy: the "fear that speech might persuade provides no lawful basis for quieting it"
  - Court holds that "information is speech" and thus that government restrictions on data collection, use and transfer must satisfy First Amendment scrutiny
  - (Note: DWT represented national advertisers in that case.)

For More Information...

- Bruce Johnson, Partner
  Chair, Privacy and Security Practice
  Davis Wright Tremaine LLP
  brucejohnson@dwt.com

- DWT Privacy and Security Law Blog:
  http://www.privsecblog.com/