PRIVACY AND DATA SECURITY

BOOT CAMP

ESPC Semi-Annual Meeting
May 13, 2015

Reed Freeman, WilmerHale

Agenda

1. Introduction to Privacy Regimes in the United States and Abroad
2. Data Security Requirements and Data Breach Response
3. Online Privacy Considerations and Regulation of Social Media
4. Financial Privacy
5. Mobile Applications and Devices
6. Marketing Restrictions
7. Health Privacy
8. Privacy and Security Considerations in Contracting
9. State Laws Imposing Additional Obligations
10. Recent Developments and Emerging Issues

Introduction to Privacy Regimes in the United States and Abroad

The United States' Sectoral Privacy Approach

- Unlike many other countries, the United States has not enacted comprehensive privacy legislation. Instead, it employs a sector-specific approach that ensures the privacy of certain types of information.
- Financial information:
  - Gramm-Leach-Bliley Act
  - Fair Credit Reporting Act
  - Right to Financial Privacy Act
  - State financial privacy laws (often stricter than their federal counterparts)
- Telephonic and electronic communications:
  - Electronic Communications Privacy Act (including Wiretap Act and Stored Communications Act)
  - Pen register and trap/trace statute
  - Computer Fraud and Abuse Act
  - Customer Proprietary Network Information statute and rules
  - State surveillance statutes

The United States' Sectoral Privacy Approach

- Video viewing information:
  - Video Privacy Protection Act
  - Cable TV Privacy Act of 1984
- Health information:
  - Health Insurance Portability and Accountability Act ("HIPAA")
  - Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- Children's information: Children's Online Privacy Protection Act
- DMV information: Driver's Privacy Protection Act
- Other "sensitive" personal information:
  - Social Security Numbers and other government-issued ID numbers
  - Biometric information (e.g., fingerprints, DNA sequences, retina scans)

Federal Trade Commission Privacy Authority

- A number of the privacy statutes discussed above give the Federal Trade Commission express rulemaking and enforcement authority.
- The FTC also has considerable power under Section 5 of the Federal Trade Commission Act, which gives the FTC authority to police "deceptive" and "unfair" trade practices.
- The FTC vigorously enforces the law, and it imposes a wide variety of sanctions on entities that violate the statutes and rules discussed above:
  - Fines and other financial penalties (for certain statutes, e.g., COPPA)
  - Burdensome auditing and monitoring obligations
  - Consent decrees with 20-year terms
  - Expansive "fencing in" sanctions, which bar violators from engaging in even lawful activities

FTC Act – "Deceptive" Trade Practices

- A practice is "deceptive" within the meaning of the FTC Act when:
  - there is a representation, omission, or practice that is likely to mislead consumers;
  - the consumers are acting reasonably under the circumstances; *and*
  - the representation, omission, or practice is material.
- **Examples include:**
  - Collecting information from consumers in a manner inconsistent with representations made in a privacy policy or elsewhere on a website
  - Omission of key facts from privacy policies
  - Sharing information with third parties despite promises to the contrary
  - Making misleading statements in advertising about your (or another's) service
  - Failing to stop all tracking when you offer an opt-out
  - Partnerships with companies that obtain data illegally
- The FTC interprets the elements of deception broadly.

FTC Act – "Unfair" Trade Practices

- A practice is "unfair" within the meaning of the FTC Act when:
  - it causes or is likely to cause substantial injury to consumers;
  - the injury is not reasonably avoidable by consumers; *and*
  - the injury is not outweighed by countervailing benefits to consumers or to competition.
- Examples include:
  - Failure to provide adequate security for personal information or sensitive personal information
  - Engaging in expansive and intrusive tracking of consumers without providing adequate notice and/or choice
- The FTC has broad authority to police "unfair" trade practices.

EU Approach – Processing of Personal Data

- "Personal data" may not be "processed" unless one of the conditions in the Directive is met.
- "Processing" is defined very broadly to include essentially anything that can be done to data, including collection, sharing with a third party, and transfer outside the EU (including *within the same company*).
- Specifically, processing is "any operation or set of operations which is performed upon personal data, … such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."
- The laws distinguish between "controllers" and "processors." The former direct the processing of data (e.g., employers with respect to employee data), while the latter process data only as instructed by the controller (e.g., cloud computing providers, payroll vendors).

EU Approach – Processing of Personal Data

- Processing is permissible only when:
  - the data subject has given his/her consent;
  - the processing is necessary for the performance of, or entering into, a contract;
  - processing is necessary for compliance with an EU legal obligation;
  - processing is necessary in order to protect the vital interests of the data subject;
  - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; *or*
  - processing is necessary for purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.
- "Necessary" is interpreted extraordinarily narrowly by EU regulators.

EU Approach – Processing of Personal Data

- *Transparency:* EU law also requires entities processing data to do so transparently. Companies must inform the "data subject" when his or her personal data is being processed and provide a wide range of information.
- *Right to object:* In most cases, companies must give the data subject an opportunity to object to the processing.
- *Access and revision rights:* Data subjects have the right to access data processed about them. And a data subject may demand revision, deletion, or blocking of data that is incomplete or inaccurate. In some cases, even accurate data must be deleted on request.
- *International transfer:* To prevent circumvention of restrictions on processing personal data, no person or company may transfer personal data to a non-EU country without complying with strict rules regulating cross-border data transfers. (This is discussed in more detail below.)
- *Member state laws:* Some countries have imposed additional limitations beyond those enumerated in the Directive.

EU Approach – Sensitive Personal Data

- Certain personal data are considered "sensitive" and are subject to even greater restrictions. They include:
  - racial or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; criminal history (including convictions or commission of offences/alleged offences).
- Some countries have specified additional categories of sensitive data.
- The rules regarding processing of sensitive data are very strict. Often, consent of the data subject is required.

Application of EU Law to US Companies

- The EU Data Protection Directive and Member States' laws apply where:
  - data processing "is carried out in the context of the activities of an establishment of the controller on the territory of the Member State"
  - an entity controlling the processing of personal data "makes use of equipment . . . situated on the territory of the . . . Member State"
- The equipment prong has been interpreted very broadly. For example, by placing a cookie on a computer, a company uses "equipment" in the EU.
- Even companies that do not trigger either the establishment or equipment prong may be subject to EU law contractually if they receive personal data from customers, suppliers, vendors, or business contacts in the EU.

Cross-Border Data Transfers – Overview

- The Data Protection Directive bars the "transfer" of personal data to any country that does not require an "adequate" level of data protection:
  - Countries deemed adequate include: Andorra, Argentina, Australia, Canada, Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay;
  - The United States' regime has *not* been deemed adequate
- The definition of "transfer" is broad; it can include merely accessing data in the United States that remains on a server in the EU.
- Certain exceptions (*i.e.*, "derogations") in the Directive permit transfers.
- In addition, a number of mechanisms exist for legitimizing data transfers to non-adequate countries, including the US-EU Safe Harbor regime, model contractual clauses, and binding corporate rules.

Cross-Border Data Transfers – Derogations

- Exceptions to the transfer prohibition include the following:
  - the data subject has given consent unambiguously to the proposed transfer
  - the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request
  - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party
  - the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of EU legal claims
  - the transfer is necessary in order to protect the vital interests of the data subject
- Again, "necessary" is interpreted extraordinarily narrowly by regulators.

Cross-Border Data Transfers – US-EU Safe Harbor

- Most U.S. companies can sign up to participate voluntarily in the US-EU Safe Harbor regime.
  - Participating companies agree to treat personal data transferred from the EU consistent with seven principles that largely track EU law: notice, choice, onward transfer, access, security, data integrity, and enforcement.
  - Companies also must satisfy a number of other requirements, including certification (and annual reaffirmation) with the U.S. Department of Commerce, compliant privacy policies and internal procedures, compliant dispute resolution procedures, annual audits, adequate security, etc.
- The Safe Harbor option is available only to companies that are subject to the jurisdiction of the FTC or Department of Transportation.

Cross-Border Data Transfers – Model Clauses

- Another option for transferring personal data from the EU is the standard (or "model") contractual clauses, which are boilerplate contracts between a data exporter and a data importer. The EU has deemed these model clauses as sufficient to ensure an adequate level of data protection.
- The EU has approved four such contracts: two for controller-to-controller transfers, and two for controller-to-processor transfers.
  - The 2004 controller-to-controller clauses are more business friendly than the 2001 version, which imposes joint and several liability.
  - The 2010 controller-to-processor clauses explicitly contemplate sub-processors, and can be used in cloud computing arrangements.
- Some countries insist on reviewing or approving model clauses contracts. This can impose a weighty burden for transfers from multiple countries.

Ongoing and Significant Changes to EU Data Privacy Law

- After the Snowden revelations, many EU Data Protection Authorities are interpreting their existing laws more strictly, especially with respect to U.S. businesses.
- These changes are especially pronounced in the cloud computing context.
- And already strict privacy laws in the European Union are poised to get even stricter through new laws.
- The existing Data Protection Directive is being replaced with a new **Data Protection Regulation** that will likely impose even greater burdens on companies both within and outside the EU.
- In theory, the new regime will replace the existing patchwork of national implementing laws with a uniform, EU-wide regulatory regime.
- There is considerable negotiation underway to revise the EU Regulation so that it is more business-friendly.

Other International Privacy Approaches

- Many countries outside of the European Union have enacted privacy regimes:
  - some are comprehensive (and strict) regimes that are patterned on the EU approach
  - others are more accurately described as "EU lite"
  - some are sectoral, similar to the U.S. approach (but often less expansive)
- Many other countries have enacted privacy laws in just the last couple of years, and it is unclear how strictly they will be interpreted and enforced.

Data Security Requirements and Data Breach Response

Data Security Overview

- There are two interrelated elements of data security:
  - *Preventative data security measures* designed to avert data breaches and other security incidents.
  - *Responsive data security measures* designed to limit the damage when preventative measures fail and a breach occurs.
- Both elements of data security are regulated at the federal, state, and international levels.
- This is a rapidly-evolving area of the law.

Consequences of Data Security Incidents

- Data security lapses have very real consequences, imposed by both regulators and the marketplace:
  - Reputational harm and loss of customers/users
  - Breach of contract
  - Burdensome public notice and remediation measures
  - Federal Trade Commission enforcement, including significant monetary penalties and burdensome audit requirements
  - State enforcement with a range of penalties
  - SEC Enforcement
  - Enforcement by international Data Protection Authorities
  - Private litigation brought by identity-theft victims and class-action plaintiffs

Federal Data Security and Breach Obligations

- There are not yet comprehensive federal rules governing data security or data incident response (though HR 1770 would do just that). Instead, there are many sector-specific laws and rules.
- "Financial institutions":
  - Gramm-Leach-Bliley Act
  - Interagency Guidelines Establishing Information Security Standards
  - Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
  - Federal Trade Commission regulations ("Safeguards Rule")
- Payment Card Industry Data Security Standard (PCI DSS)
  - Industry standard requiring entities handling bank cards to conform to rigorous security standards and certain requirements for testing and reporting
  - Failure to comply can result in fines and other serious penalties

Federal Data Security and Breach Obligations

- Communications sector:
  - Cable TV Privacy Act of 1984
  - Customer Proprietary Network Information rules
- Children's Online Privacy Protection Act
- Health sector:
  - HIPAA – Health Insurance Portability and Accountability Act
  - HITECH Act – Health Information Technology for Economic and Clinical Health Act
  - HHS and FTC rules
- Other legal requirements that apply to companies in *any industry sector*:
  - Obligations stemming from contracts
  - Securities and Exchange Commission reporting obligations
  - Federal Trade Commission enforcement of data security through its authority to police "unfair" or "deceptive" trade practices

State Data Security Obligations

- Many states mandate preventative data-security measures.
- The protected information generally falls into the same categories discussed above, such as financial information and health information.
- Massachusetts data security statute and rules (201 C.M.R. 17.00 *et seq.*):
  - Apply to *any entity* with sensitive personal information about Massachusetts consumers (e.g., social security numbers, state ID numbers, financial information)
  - Require a *written* information security program
  - Require entities to execute contracts with vendors and other service providers to ensure that third parties take adequate security measures
  - Impose specific requirements with respect to computerized information, including encryption of portable devices and certain electronic transmissions, specific access controls, firewalls, and malware protection

State Data Breach Response Laws

- Nearly all states have data breach notice and response laws
- These laws generally have extraterritorial effect and thus can apply to data breaches occurring *anywhere*, and even to out-of-state companies, so long as they possess certain types of data about state residents
- These laws differ markedly in their scope and application:
  - *Types of data covered* — from social security numbers to financial data to fingerprints to health insurance information to birthdates
  - *Forms of protected data* — computerized vs. hard copy
  - *Risk triggers* — potential for harm from breach often (but not always) required
  - *Required responses* — from consumer notice to alerting state agencies and credit bureaus
  - *Exclusions and limitations* — e.g., entities regulated under Gramm-Leach-Bliley

International Data Breach Laws

- This is one area where U.S. law is stricter than that of many other countries around the world.
- The rest of the world is catching up, however, and many other countries have recently adopted data breach reporting laws.
- Many others are currently contemplating data breach reporting laws.
- The proposed EU Regulation includes a strict data breach reporting requirement.

Data Security and Corporate Governance

- "Voluntary" frameworks and "best practice" standards are fast establishing a standard of care.
- Companies should develop a written information security program tailored to the complexity of their business and the sensitivity of their data.
- **Technical safeguards**
  - **Virus protection, firewalls, software patches, robust passwords, encryption, audit procedures, etc.**
- **Physical safeguards**
  - **Clean desk policy, secured workstations, locked filing cabinets, etc.**
- **Organizational safeguards**
  - **Chief Privacy Officer, need-to-know data access, termination of privileges for separated employees, effective disciplinary procedures, employee vetting, service provider oversight, etc.**

Planning for Incident Response – Practical Tips

The following steps should be taken to prepare for a data security incident before it happens.

- Written security incident response plan:
  - Identify 24/7 points of contact
  - Establish clear roles and responsibilities
  - Provide escalation procedures
  - Account for different types of incidents
  - Give guidance on responding to customers, business partners, press, regulators, and others
  - Reflect federal, state, and international notice and reporting requirements
- Tabletop exercises or roleplaying a simulated breach.
- Negotiation of engagement terms with data forensics firm(s).
- Engagement of other vendors necessary for effective breach response.

Online Privacy Considerations and Regulation of Social Media

Online & Offline Tracking and Profiling

- Consumers are pervasively tracked online through cookies, web beacons, flash cookies, browser fingerprinting, device IDs, social media plugins, JavaScript, and now cross-device
- Keys:
  - Privacy representations: Must be accurate and complete
  - Surprise: Just-in time notice
  - Sentitive: Opt-in
  - Understand where data came from and what restrictions come with it.
  - Opt-Out must be complete

Mobile Applications and Devices

California Is Leading the Charge on Mobile Privacy

- California has stepped up enforcement of the California Online Privacy Protection Act against companies that offer mobile apps.
  - For a decade, California law has required Internet websites to provide an online privacy policy. *See* Cal. Bus. & Prof. Code §§ 22575 *et seq.*
  - Authorities have clarified that the law applies to mobile applications too.
  - After many companies ignored that pronouncement, California sent scores of letters notifying companies that their mobile applications did not comply with the statute.
  - The response of Delta Airlines, which provides a "Fly Delta" mobile application, did not satisfy California regulators. So the California Attorney General filed suit, seeking a potential penalty of $2,500 per download.
  - The case was dismissed on airline preemption grounds and is now on appeal; California AG may seek new defendant.

California's Mobile Privacy Recommendations

- In 2013, California issued a lengthy report analyzing the mobile ecosystem and making privacy recommendations for app developers, app platform providers (*e.g.*, app stores), advertising networks, and others.
  - *Privacy on the Go: Recommendations for the Mobile Ecosystem* (2013), http://www.oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf?
- Some of the recommendations in the California report go beyond existing law and are merely "best practices" rather than legal requirements.

California's Mobile Privacy Recommendations

- Key recommendations in the California report include:
  - Making privacy policies available to consumers before they download an app.
  - Using shorter privacy disclosures and other measures to draw users' attention to data practices that may be unexpected.
  - Minimizing collection of personally identifiable data that is not necessary for the basic functions of the app.
  - Enabling consumers to make meaningful choices about the collection and use of their data and avoiding "take-it-or-leave-it" choices.
  - Augmenting privacy disclosures when collecting sensitive data, text messages, call logs, contacts, or privacy-sensitive device features (*e.g.*, cameras, microphones).
  - Avoiding using (or obtaining informed prior consent for) out-of-app ads delivered by modifying browser settings or placing icons on the mobile desktop.
  - Moving away from the use of device-specific identifiers for advertising and transitioning to app-specific or temporary device identifiers.

Efforts by the Federal Trade Commission

- The Federal Trade Commission also is addressing thorny issues in the mobile ecosystem.
  - Federal Trade Commission, Marketing Your Mobile App (Aug. 2012)
  - Federal Trade Commission, Mobile Privacy Disclosures: Building Trust Through Transparency (Feb. 2013)
- The FTC is grappling with many of the same issues discussed above. In addition, it is addressing such issues as:
  - Geo-location data.
  - Tracking of mobile device use for behavioral advertising and other purposes.
  - Reliance on third-party toolkits.
  - Excessive data collection.
  - Fair Credit Reporting Act obligations.
  - Mobile applications that collect children's information.

Marketing Restrictions

Marketing Emails, Text Messages, and Phone Calls

- **CAN-SPAM**. Governs the marking and content of "commercial messages" (emails with primary purpose of commercial advertisement/promotion).
  - Mandatory notice/opt-out mechanism for commercial promotional e-mail
  - Exceptions for transactional & relationship messages
- **Canada's Anti-Spam Legislation**. Applies to commercial electronic messages sent to an electronic address.
- **TCPA**. Restricts telemarketing and the use of automated telephone equipment for voice messages, text messages, and faxes.
  - Consent required for text messages and automated calls
  - Requirements vary depending on relationship with consumer and message
- **Telemarketing Sales Rule**. Regulates calls by any plan, program, or campaign to sell goods or services through phone calls to consumers.

Health and Medical Privacy

Health and Medical Privacy

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- Key elements
  - Safeguards for identifiable health data handled by health plans, providers, clearinghouses, and their business associates
  - Privacy Rule: Notice, choice (opt in/opt out), access, amendment & accounting of disclosures for uses and sharing other than treatment, payment, and administrative operations
  - Security Rule: Physical, administrative, technical security safeguards for electronic health data
  - Breach Notification Rule: Mandatory notice and reporting of breaches of unsecured identifiable health data
  - Business Associate Contracts
- State and foreign health privacy laws.

Privacy and Security Considerations in Contracting

Issues Arising in Third-Party Contracts

- Privacy, confidentiality, and security clauses now are heavily negotiated provisions in most third-party contracts, especially outsourcing agreements. And some statutes and regulations require specific contractual provisions.
- All regulatory guidance has a consistent theme: while functions may be outsourced, accountability remains with the outsourcing entity.
- Many technology vendors are becoming more aware of the changing environment and as a result are more risk averse.
  - Liability caps and disclaimers of certain types of liability
  - Costs associated with complying with changes in the law
- By contrast, companies outsourcing data have sought certain protections.
  - Customer audits/access to logs
  - Data deletion
  - Downtime credits/indemnification
  - Encryption

Privacy Concerns When Using the Cloud

Many countries have expressed concern about companies' ability to fulfill their privacy duties when moving data to the cloud.

- The European Union has been particularly vocal in articulating concerns about the privacy implications of cloud computing.
  - *See, e.g.,* Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP 196, 01037/12/EN (July 1, 2012).
- EU regulators have identified some additional privacy concerns in the cloud context that correspond to the privacy rights afforded to data subjects under EU law:
  - Access and correction rights
  - Right to be forgotten / deletion rights
  - Data portability
  - Limitations on trans-border data flows
  - Data retention

State Laws Imposing Additional Obligations

State Privacy and Security Laws

- Shine the Light Act
- Song-Beverly Credit Card Act and similar state laws
  - Zip code class-action litigation
- California Online Privacy Protection Act
  - New "do not track" disclosures
- Safeguarding personal information:
  - 201 C.M.R. § 17.00 *et seq.*
  - N.Y. Gen. Bus. Law § 399-dd(1)
  - Cal. Civ. Code § 1798.85
  - Driver's license barcode data
- Electronic eavesdropping and surveillance:
  - Single party consent
  - All party consent

Thank You and Contact Information

Reed Freeman
Partner
WilmerHale

+1 202 663 6267
Reed.freeman@wilmerhale.com