PRIVACY AND DATA SECURITY

Union Square Ventures — April 18, 2013

Heather Zachary, WilmerHale

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Overview

1. Introduction to Privacy Regimes in the United States and Abroad
2. Mobile Applications and Devices
3. Lawful Collection and Use of "Big Data"
4. International Privacy and Cross-Border Data Transfers
5. Data Security Requirements and Data Breach Response
6. IT Outsourcing and the Cloud
7. 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
  - State financial privacy laws (often stricter than their federal counterparts)
- Telephonic and electronic communications:
  - Wiretap Act
  - Electronic Communications Privacy Act
  - Stored Communications Act
  - Computer Fraud and Abuse Act
  - Pen register and trap/trace statute
  - 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

- Several 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
  - 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 trade 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
  - Sharing information with third parties despite promises to the contrary
  - Making misleading statements in advertising about your (or another's) service
- The FTC interprets the elements of deception broadly.

FTC Act – "Unfair" Trade Practices

- A trade 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 sensitive consumer data
  - 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

The European Union's Comprehensive Privacy Approach

- The European Union has a strict privacy regime that comprehensively regulates a far wider range of information than is protected in the US.
- The EU has interpreted its privacy laws to have broad extraterritorial effect, so even US-only companies often must take steps to comply.
- The EU enacted its overarching "Data Protection Directive" in 1995 (95/46/EC), and it has since been implemented through the privacy laws of each individual Member State.
- The scope of data protected by the Directive is extraordinarily broad:
  - "Personal data" is defined as "any information relating to an identified or identifiable natural person …; an identifiable person is one who can be identified, directly or indirectly, … by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."
  - Even a person's email address, photo, work phone number, or IP address is considered "personal data" that is subject to significant protections.

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 extraordinarily broadly to include essentially anything that can be done to information, including collection and sharing.
- 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."

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 a 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.

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 the revision, deletion, or blocking of data that is incomplete, inaccurate, or is not being processed in compliance with applicable data protection laws.
- *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.
- *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)

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.

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 nearly a decade, California law has required Internet websites to provide an online privacy policy. *See* Cal. Bus. & Prof. Code §§ 22575 *et seq.*
- Authorities recently clarified that the law applies to mobile applications too.
- After many companies ignored that pronouncement, California sent scores of letters in late 2012 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 on December 6, 2012. Delta now faces a potential penalty of $2,500 per download.

California Initiatives Concerning Privacy Policies

- California has enlisted the major app store providers in its efforts. In February 2012, Amazon, Apple, Google, Hewlett-Packard, Microsoft, and Research in Motion signed an agreement with the California AG committing to make it easier for apps providers to post privacy policies that consumers can review before downloading mobile apps.
  - Facebook signed the agreement in June.
- Some companies are using the same privacy policy for their mobile applications as for their Internet websites. This is a dangerous practice.
  - Online behavioral advertising opt-outs.
  - Small screens on mobile devices.
  - Different practices for collection, use, or sharing of data collected though mobile apps.

California's Mobile Privacy Recommendations

- On January 18, 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.

California's Mobile Privacy Recommendations

- The California report has garnered criticism from some important members of the mobile ecosystem.
  - Industry groups have criticized the recommendations, arguing that they clash with developing industry standards and have no basis in existing law.
- Mobile app providers that ignore the report do so at their peril. California created a new Privacy Enforcement and Protection Unit in July 2012, and mobile privacy is clearly a key priority for the unit.

Efforts by the Federal Trade Commission and Industry Stakeholders

- The Federal Trade Commission and industry stakeholders are also 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)
  - NTIA Multistakeholder Process
- The FTC and industry stakeholders are grappling with many of the same issues discussed above. In addition, they are 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.

Mobile Payments Issues

- Mobile payments present challenging privacy compliance issues due to the intersection of the financial services industry, which is heavily regulated, with the far more freewheeling mobile applications industry.
- Key mobile payments challenges include:
  - Compliance with financial privacy statutes and rules that were enacted long before the emergence of mobile payments.
  - Effective disclosure of privacy policies and regulator-mandated notices on the small screens of mobile devices.
  - Keeping information secure when a mobile phone is lost or stolen.
  - Keeping data secure as it is transferred from a consumer to the recipient.
- Recent statements by regulators suggest that the industry should expect increased FTC attention to mobile payment issues in the coming year.

Lawful Collection and Use of "Big Data"

The Promises of "Big Data"

- What is "big data"?
- Big data holds great promise for both businesses and consumers.
  - Analytics performed on a database of 1.4 million Kaiser Permanente members revealed that Vioxx—a popular pain reliever—was responsible for tens of thousands of cardiac arrest deaths.
  - Analysis of big data helps governments manage traffic congestion and helps utilities design smart-grid systems that increase energy efficiency.
  - Big data enables businesses to better manage supply chains and helps provide significant insights into consumer behavior.
  - Big data also helps reduce risk in the financial sector by identifying the characteristics of borrowers who are most likely to default.

The Perils of "Big Data"

- Big data also presents potential privacy perils.
- These dangers are not merely "bigger"; they can also be different in kind.
  - The risk of re-identification of "de-identified" data is particularly high with respect to big data.
  - Big data frequently involves combining information from a variety of sources, and that information can be subject to differing privacy obligations.
  - Big data enables companies to engage in consumer profiling, or "weblining."
  - Big data is often used for far different purposes than it was collected for.
  - Big data creates incentives to collect more information and retain it longer.
  - More intrusive and surprising tracking is possible with big data collection.
  - Big data can involve the combination of information collected online and offline.
  - Big data presents greater data-security risks because larger and more comprehensive databases are more attractive to hackers.

Increased Government Attention on Collectors and Users of Big Data

- Regulators and lawmakers have focused their attention on big data in recent months.
- Large data brokers have been a focus of significant activity:
  - In late 2012, several members of Congress initiated investigations into the practices of certain data brokers. Among other things, they sent letters to data brokers requesting detailed information about their data collection, use, and transfer practices.
  - In December 2012, the Federal Trade Commission followed suit, issuing administrative subpoenas to nine data brokers. The subpoenas require each company to provide extensive details about its practices.
- In its March 2012 Privacy Report, the FTC also called for legislation to provide greater transparency of, and consumer control over, practices of data brokers.

Increased Government Attention on Collectors and Users of Big Data

- The FTC has also focused special attention on a broader category of "large platform providers."
  - These companies include Internet service providers, operating systems, browsers, and social media networks.
- These developments are relevant to all participants in the Internet ecosystem, including small companies.
- The FTC and state regulators have not limited their attention to the large data brokers that collect and disseminate information about consumers.
  - In its March 2012 privacy report, the FTC outlined best practices for ***all*** companies that collect, use, and transfer consumer data.
  - Recent enforcement actions have demonstrated that the FTC is focused on protection of personal data as it travels throughout the online ecosystem.

Additional Considerations for Small and Mid-Sized Companies Leveraging Big Data

- Small and mid-sized companies are increasingly looking to leverage the data they have collected themselves or obtained from other companies, but the legal landscape is complex and rapidly changing.
- These companies should ensure compliance with a variety of federal laws:
  - Federal Trade Commission Act
  - Gramm-Leach-Bliley Act
  - The Wiretap Act and the Electronic Communications Privacy Act
- A multitude of state laws apply as well.
  - State analogues to the FTC Act and Gramm-Leach-Bliley Act
  - Limitations on collection and use of sensitive information (including social security numbers, drivers' license numbers, financial data, health data, etc.)
  - State surveillance statutes, including those requiring two-party consent
  - Data breach reporting and notification laws

International Privacy and Cross-Border Data Transfers

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 legal claims
  - the transfer is necessary in order to protect the vital interests of the data subject

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.
- Some countries insist on reviewing or approving model clauses contracts. This can impose a weighty burden for transfers from multiple countries.

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
  - 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 no comprehensive federal rules governing data security or data incident response. Instead, there are many sector-specific laws and rules.
- "Financial institutions":
  - Gramm-Leach-Bliley Act
  - Federal Trade Commission regulations ("Safeguards Rule")
  - Interagency Guidelines Establishing Information Security Standards
  - Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- Payment Card Industry Data Security Standard (PCI DSS)
  - Industry regulation 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" 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. Of particular note are social security numbers, which many states protect.
- Massachusetts data security statute and rules (207 CMR 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 Security Obligations

- The European Union Data Protection Directive requires entities that manage personal data to employ appropriate technological and organizational measures to ensure the security of that data.
- Different countries in the EU have implemented this requirement in different ways.
- A number of non-EU countries have adopted specific data-security requirements as well.

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

- Develop a written information security program tailored to the complexity of your business and the sensitivity of your 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.
- Incident response planning and practice

Planning for Incident Response – Practical Tips

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

- Anticipate Various Incident Types: Develop tailored procedures for handling different types of information security incidents
- Analytic Capacity: Develop means of analyzing and identifying the incident's cause
- Clear Documentation Requirements: Outline steps for gathering information and documenting the incident
- Escalation of Serious Intrusions: Develop criteria for prioritizing incidents and assessing the criticality of the affected resources
- Mechanism to Mandate Corrective Action: Develop procedures for planning and implementing corrective steps
- Communication Protocols: Draft procedures for communication with those affected by or involved with recovery from the incident
- Forensics: Ensure proper collection and preservation of audit trails/other evidence

IT Outsourcing and "the Cloud"

Cloud Definitions

FFIEC: "In general, cloud computing is a migration from owned resources to shared resources in which client users receive information technology services, on demand, from third-party service providers via the Internet 'cloud.'"

Models:

- Infrastructure as a Service (IaaS): data center hardware
- Platform as a Service (PaaS): database environment
- Software as a Service (SaaS): software applications

Pros and cons of getting computing services over the Internet:

- Resource pooling
- Broad network access
- Rapid elasticity
- Measured service
- Loss of control over location, security of data

Privacy Considerations When Using the Cloud

Cloud computing can also give rise to privacy concerns. These concerns are related to, but distinct from, data-security concerns.

- Providers of cloud computing services often employ sub-processors.
- Cloud arrangements can be less transparent to consumers.
- Data stored in the cloud can be physically located in, or electronically accessible from, countries with vastly different privacy laws.
- Individual companies' privacy policies might not be consistent with certain types of cloud computing arrangements.
- Companies handling financial data must ensure that their use of the cloud complies with the Gramm-Leach-Bliley Act and state analogues.

International Privacy Concerns

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 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
- This year, EU regulators are expected to issue model contracts for cloud computing designed to ensure adequate privacy protections.

Issues Arising in Third-Party Contracts

- All regulatory guidance has a consistent theme: while functions may be outsourced, accountability remains with the outsourcing entity
- Privacy, Confidentiality, and Security Clauses now are heavily negotiated provisions in outsourcing agreements
- 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

Recent Developments and Emerging Issues

Significant Changes to EU Data Privacy Law

- Already strict privacy laws in the European Union are poised to get even stricter.
- 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.
- The new regime will replace the existing patchwork of national implementing laws with a uniform, EU-wide regulatory regime.
- EU law would apply directly to many US-based companies, including those without a physical presence in the EU. Specifically, the regulation would apply to non-EU companies that process data related to the:
  - "offering of goods or services" to EU residents, or
  - the "monitoring of their behaviour."

Significant Changes to EU Data Privacy Law

- Other key elements of the proposed EU Regulation include:
  - Right to data portability.
  - Right to be forgotten.
  - Hefty fines for violations.
- A draft report issued earlier this year by a rapporteur for one of the European Parliament's prominent committees proposed amendments that would make the EU Regulation even stricter in some respects.
- There is considerable negotiation underway to revise the EU Regulation so that it is more business-friendly.
- According to the European Commission, a vote in the Parliament on the Amendments is expected later this year, and a final agreement between the Parliament and the Council could occur by late 2013. Many view that timeline as ambitious.

EU "Cookie Directive"

- There is potential for increased enforcement of the EU "Cookie Directive." (Directive 2009/135/EC)
  - The extraterritorial reach of the Cookie Directive is remarkable.
  - In some countries, certain types of cookies require affirmative, opt-in consent.
  - Many countries require banner warnings or website overlays and clear notice to consumers regarding cookies.
  - Many U.S. companies are not yet in compliance with the directive.

United States: New COPPA Rules

- The FTC recently adopted new rules implementing the Children's Online Privacy Protection Act. Compliance is required by July 1, 2013.
- Key rule changes:
  - Strict liability standard for websites and other online services that enable third-party providers operating on their website or service (such as applications, plug-ins, or advertising networks) that collect personal information from users of the website or service
  - Additional ways to obtain "verifiable parental consent" for the collection, use, and disclosure of children's personal information
  - The definition of "personal information" encompasses a wider range of information, including persistent identifiers
  - Websites and other online services that are "directed to children" but that do not target children as their primary audience will be permitted to age-screen their users and apply COPPA's protections to only those users who self-identify as under age 13

Thank You and Contact Information

Heather Zachary
Partner
WilmerHale

+1 202 663 6794
Heather.Zachary@wilmerhale.com
http://www.wilmerhale.com/Heather_Zachary/