FinTech Webinar Series:

CYBERSECURITY AND DATA PRIVACY UPDATE

Jonathan Cedarbaum, Robert Finkel, and Heather Zachary

October 23, 2013

WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Speakers

Jonathan G. Cedarbaum
Partner
WilmerHale

Robert Finkel
Partner
WilmerHale

Heather Zachary
Partner
WilmerHale

Overview

1. Recent Federal Cybersecurity Developments: Executive Order, NIST Standards, Information-Sharing, Legislation
2. Privacy and Security Issues in Cloud Computing Contracts
3. International Privacy and Transferring Data Across Borders
4. Mobile Devices and Mobile Apps
5. Workplace and Corporate Governance Developments
6. The FTC's New Rules Concerning Children's Privacy

Recent Federal Cybersecurity Developments

Executive Order 13636 (Feb. 12, 2013)

- Directs the National Institute of Standards and Technology ("NIST"), through a consultative process with other agencies and CI owners and operators, to develop cybersecurity performance standards and methods to reduce risks to CI ("Cybersecurity Framework")
- Directs DHS and agencies responsible for CI sectors to create a program to encourage CI owners and operators to voluntarily adopt the Cybersecurity Framework established by NIST
- Directs agencies that have statutory authority to regulate CI to determine whether they have "clear authority" to establish mandatory standards based on the Cybersecurity Framework and, if current regulatory requirements are deemed insufficient, to impose such standards through rulemaking
- Expands to all CI sectors the Enhanced Cybersecurity Services Program and requires key federal agencies to provide more cybersecurity threat information to CI owners
- Instructs GSA and DoD to look into incorporating cybersecurity standards into federal acquisition and procurement policies
- Requires an annual report to the President about the extent to which CI owners and operators are participating in the voluntary program.

Preliminary NIST Cybersecurity Framework

- Preliminary version released October 22, 2013: http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf
  - 45-day comment period coming
  - Final version to be released in February 2014
- Emphasizes **risk-management** approach to cybersecurity efforts
- Divides Framework into three parts: Core, Profile, Implementation Tiers
- Core: five functions
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- For each, categories, e.g., Asset Management, and subcategories, e.g., inventorying of software platforms and applications
- Profile: establishing an organizational road map to get from here to there, i.e., substantially reduced cyber risks
- Implementation Tiers: (i) partial; (ii) risk-informed; (iii) risk-informed and repeatable; (iv) adaptive

Preliminary NIST Cybersecurity Framework

- Six-step process for establishing or improving a cybersecurity program
- Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Progam
  - Quite detailed outline of best practices for handling PII
  - Legal basis, effects not always clear
- Issues for further development:
  - (i) authentication;
  - (ii) automated indicator sharing;
  - (iii) conformity assessment;
  - (iv) data analytics;
  - (v) international aspects, impacts, and alignment;
  - (vi) privacy; and
  - (vii) supply chains and interdependencies

- Fifth public workshop, Nov. 14-15, N.C. State, Raleigh

Voluntary Program Development

- **Incentives Reports by DHS, Commerce, Treasury:**
  - Better information-sharing
  - Liability protection, conditioned on adequate insurance coverage?
  - Technical assistance and training
  - Grants or, for regulated industries, rate recovery
- **Stakeholder meetings led by DHS:**
  - September 23, October 21?, November 18?
  - Efforts to clarify what is involved in implementation/adoption
    - Guidance for sector-specific agencies
    - Guidance for companies and trade associations or other private-sector collaborations

Information-Sharing

- **Enhanced Cybersecurity Services ("ECS") Program**
  - From 2010 Defense Industrial Base ("DIB") Pilot
  - New, All-Sector ECS:
  - Companies must apply to be approved by DHS or SSA as a "critical infrastructure entity"
  - Approved commercial service providers ("CSPs) receive threat information from DHS, which they can use to protect their customers
  - If customer agrees, CSP may also share anonymized threat information back with the Government
- **Other Efforts**
  - Treasury Cyber Intelligence Group
  - E.O. directive that DOJ, ODNI, DHS issue instructions for timely production of unclassified reports on cyber threats to targets of the threats
  - FS-ISAC
  - Regional Exchanges
- **Liability concerns from monitoring and information-sharing:**
- **Legislative responses?**

Privacy and Security Issues in Cloud Computing Contracts

Privacy and Security Issues in Cloud Contracts

- **General Regulatory Guidance**
  - Functions may be outsourced, accountability remains with management and Board
- **Recent FFIEC Heightened Interest**
  - Cloud Computing Statement (July 10, 2012): Cloud as just another form of outsourcing, but more robust controls may be necessary given Cloud's nature
  - Revisions to *IT Exam Handbook*; further revisions expected shortly from Cybersecurity and Critical Infrastructure Committee
  - Issuance of *Administrative Guidelines on Implementation of Interagency Programs for the Supervision of Technology Service Providers* (October 2012)
- **Possible Tensions Between Cloud Model and Regulatory Approach?**
  - Guidance is technology agnostic: rules apply regardless of the form of outsourcing
  - Industry vendors often approach cloud services as non-customized, uniform service offerings, different in kind than traditional outsourcing models

Privacy and Security Issues in Cloud Contracts

- **Financial Institution Must Conduct Proper Due Diligence**
  - Sensitivity of Data and Protective Controls
  - Data Segregation , including controls on Integrity and Confidentiality of Data
  - Recoverability, including how vendor will respond to disasters

- **Information Security**
  - Continuous Monitoring if high-risk situation
  - Cloud Services increase need for encryption and access controls
  - Incident Response Methodologies
  - Strategies for investigation and forensic collection.

Privacy and Security Issues in Cloud Contracts

- **Robust Termination Rights**
  - Removal or Deletion of Data at the end of the Contract, regardless of location; Risk may be higher than in traditional outsourcing
  - Right to assign contract to acquirer or in a workout situation

- **Other Key Contract Terms**
  - Prompt Reporting and Remediation of Security Breaches
  - Liability caps and disclaimers of certain types of liability
  - Vendor monitoring of legislative and regulatory changes
  - Costs associated with complying with changes in the law

Contracting Considerations for EU Data

- Though the EU Data Protection Authorities have differing views, increasingly they have been adopting the position of the Article 29 Working Party.
  - Opinion 05/2012 on Cloud Computing, WP 196, 01037/12/EN (July 1, 2012).
- The Opinion mandates transparency in cloud computing contracts. Specifically, it states that the cloud provider should disclose to clients:
  - all locations where data will be stored; and
  - the identities of the cloud provider's subcontractors.
- The Opinion requires the client to control its data. The contract should:
  - bar the cloud provider from processing data for its own purposes;
  - give the client power to approve all subcontractors or terminate the contract;
  - enable the client to seek a remedy for subcontractors' privacy violations; and
  - require the cloud provider to notify the client of any requests by government entities for data, unless such notification is prohibited by law.

Contracting Considerations for EU Data

- If the cloud provider will transfer data from the EU to elsewhere, the parties must ensure that some mechanism is in place to legitimize the initial transfer and all onward transfers of the data.
  - Examples include the Safe Harbor (controversial), or "model" contractual clauses.
- The contract should require the cloud provider to implement adequate technical and organizational measures to protect any personal data.
  - This is required under Article 17 of the Data Protection Directive as well.
- There should be adequate safeguards to ensure that the cloud provider does not retain any data that the cloud client decides to delete.
- The cloud provider must cooperate with the client to ensure that individuals' access, correction, and deletion rights are protected.
- Some EU ***financial regulators*** insist on even greater contractual safeguards, such as audit rights for the client or an examination right for the regulator.

National Financial Regulators

- Increased interest by financial regulatory authorities in many countries
  - Statements on Cloud use: Netherlands, Belgium, Canada, France
  - Statements/guidance in the works?: France, Luxembourg, Japan, China, South Korea

- Some trends:
  - Some jurisdictions, like the U.S., approach as risk-management issue to be incorporated in larger risk-management, outsourcing guidance
  - But even among some of those, as in U.S., heightened concern, possibility of regulatory expectations inconsistent with particular data handling practices
  - Recent regulatory steps to investigate:
    - Regulatory approval or notification, at least for important operational functions
    - Audit rights, by regulator or financial institution
    - Specified contract clauses, e.g., re information access,
    - Customer consent
  - Some jurisdictions more hostile, esp. concerned about data containing customer personal financial information being held outside national boundaries: South Korea, Singapore?, Luxembourg?, Switzerland?

- Crucial to investigate particular regulatory requirements country by country

International Privacy and Transferring Data Across Borders

Post-Snowden Controversies Concerning the Adequacy of Mechanisms for Protecting EU Data in the United States

- The U.S.-EU Safe Harbor regime has always been controversial with the more conservative Data Protection Authorities in the EU, and criticism of it has reached new heights recently.
  - Several negative reports and guidance documents from DPAs and the European Parliament.
  - Proposals to sunset the Safe Harbor immediately or as part of the Data Protection Regulation.
- Though no formal changes have been made, conservative DPAs have made some headway against the Safe Harbor in the context of *service provider relationships*. This already is having a direct impact on FinTech companies that partner with companies in the EU.
  - DPAs and others argue that the Safe Harbor cannot legitimize transfers from a "controller" in the EU to a "processor" in the United States (and especially "onward transfers" from the processor).
- The U.S. Department of Commerce has vigorously resisted such attacks on the Safe Harbor.
  - One helpful document is Dep't Commerce, "Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing." (Apr. 2013). Though it focuses on cloud computing, it has clear application to any controller-processor arrangement that a FinTech company might enter into.
- Many FinTech companies are also facing misconceptions about the PATRIOT Act. Dispelling these (where possible) has been very important to these companies' bottom lines.

New Guidance on the EU "Cookie Directive"

- Considerable divergence remains in countries' interpretations. Some permit an opt-out approach, while others mandate an opt-in approach for certain types of cookies.
- A paper from the Article 29 Working Party puts more pressure on companies to use robust forms of consent. It says consent mechanisms should have four elements:
  - Working Document 02/2013 providing guidance on obtaining consent for cookies, WP 208, 1676/13/EN (Oct. 2, 2013)
  - **"Specific information"** — Users must receive "clear, comprehensive, and visible notice" about the cookies used and their purposes (including any third-party cookies or access to cookie data).
  - **"Timing"** — Consent should be obtained before cookies "are set or read," unless an exception to consent applies.
  - **"Active behavior"** — Consent must be unambiguous, shown through "an active indication of the user's wishes." For example, clicking on a button or link, ticking a box, or "any other active behavior from which a website operator can unambiguously conclude" the user has consented.
  - **"Real choice"** — Consent can be valid only if the user has real choice. An operator should not condition general access to sites on the acceptance of all cookies (e.g., e-commerce site). Users should be given meaningful choice concerning cookies that are not needed for site functioning.

Status of the New Data Protection "Regulation"

- The already strict data protection laws in the EU are likely to become even stricter under the Data Protection Regulation being negotiated.
- Procedural status of the Regulation:
  - The regulation has been subject to thousands of amendments over the last few months. Those amendments were voted on ***just this Monday*** by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.
  - The draft will weave its way through the EU apparatus, potentially going to a Conciliation Committee if agreement cannot be reached. Ultimately, the Council of the European Union, European Parliament, and European Commission must collaborate on a draft, which will be adopted and signed into law.
  - The Parliament is pushing to get an agreement before the May 2014 elections. If they don't meet that deadline, there will be significant delays, and the adoption of any new Regulation could be in jeopardy.
  - Even after the Regulation is enacted, it will not be effective for another two years.

Status of the New Data Protection "Regulation"

- The substance of the Regulation remains much in flux. However, the following provisions (and many more) are included at this time:
  - **Hefty fines.** A company could face significant fines from EU regulators. Under the current draft, fines for some violations could amount to ***100 million euros*** or ***five percent of a company's annual worldwide turnover***, whichever is ***greater.***
  - **"Anti-FISA" provision.** This element of the Regulation was added recently. It had been included in an earlier draft of the Regulation, but was removed after heavy lobbying by the United States. After the Snowden revelations, it was reinserted. This provision could put U.S. companies in the position of choosing to violate either U.S. law or EU law.
  - **"Right to erasure."** This was originally the "right to be forgotten." Though still under debate, it would require erasure of data on request and communication of such requests to third parties.
  - **"One-stop-shop" principle.** This would allow organizations in the EU to report to just one data protection authority (their home authority) rather than one (or more) in each EU member state. That home DPA could issue decisions that are binding throughout the EU. There is currently debate as to how much influence other DPAs should have with respect to such decisions, and whether decisions should be reviewable by an independent panel.

Mobile Devices and Mobile Apps

Updates to the California Online Privacy Protection Act

There have been important developments concerning the California Online Privacy Protection Act, which applies to mobile apps.

- The statute requires providers of websites and online services to disclose a privacy policy to consumers. *See* Cal. Bus. & Prof. Code §§ 22575 *et seq.*
- The California AG's CalOPPA litigation against Delta Airlines was dismissed for non-privacy reasons. Such litigation could be brought against a new target.
- The legislature amended CalOPPA to require disclosure of more information:
  - "whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service." California A.B. 370 (Sept. 27, 2013).
  - "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."

NTIA Multi-Stakeholder Process

- After a year of meetings among industry, consumer advocates, and government representatives, the NTIA multi-stakeholder negotiations on mobile app transparency yielded a self-regulatory code of conduct.
- The outcome is controversial. Some industry groups (including the Direct Marketing Association) and some consumer groups are unhappy with the result.
- The code is voluntary, but for those app developers that do adopt it, it requires short-form notices that supplement more traditional, longer-form privacy policies. The notices must (subject to limited exceptions):
  - disclose the identity of the entity providing the app;
  - explain whether the following data are collected: biometrics; contacts; financial, health, medical, or therapy info; browser history; call or text logs; location; or user files on the device;
  - disclose whether data are shared with ad networks, mobile carriers, data resellers, data analytics providers, government entities, operating systems/platforms, other apps, or social networks;
  - describe a means of accessing a long form privacy policy, if any exists; and
  - where practicable, be provided prior to download or purchase of the app.
- Even though the code is voluntary, it could influence mandatory regimes.

Mobile Apps and Payments

- A number of issues arise in the mobile payments context due to the intersection of the heavily regulated financial industry with the anything-goes mobile app culture.
- One key issue for mobile payments providers is the appropriate policies:
  - Gramm-Leach-Bliley privacy statement
  - Online privacy policy
  - Short-form mobile app policy
  - Other consumer notices required by financial statutes and regulations
- Another issue is E-SIGN Act compliance. Required notices can be provided electronically so long as specific procedures are followed.
- Though similar in substance, the legal basis for security requirements varies depending on the type of entity involved, as does the specificity of the guidance.
  - Interagency Guidelines issued by the federal functional regulators
  - FTC Safeguards Rule
  - Federal Trade Commission Act
  - State data security laws (e.g., Massachusetts)

Mobile Security

- Explosion of reliance on mobile devices
  - 25% of e-commerce Q1 of 2013 as compared to 2% just two years earlier
  - Smartphone use average of 150 times/day
- Rise of B.Y.O.D.: Personally owned smart phones, tablets, other mobile devices used in enterprises now outnumber company-issued counterparts two to one?
- Some top threats:
  - Lost, stolen, decommissioned devices; Symantec Honey Stick Project
  - Information-stealing malware; especially Android apps
  - Data loss/leakage through poorly designed apps
  - Vulnerabilities within devices, including insufficient management tools
  - Unsecured WiFi, network access, rogue access points
- Increased FTC Scrutiny
  - Mobile Security Forum, June 2013
  - More enforcement activity: e.g., HTC America settlement, Feb. 2013
  - *Mobile App Developers: Start with Security* (Feb. 2013)

Workplace and Corporate Governance Developments

FFIEC Social Media Guidance

- Draft guidance issued January 2013 (78 Fed. Reg. 4848 (Jan. 23, 2013))
- FIs "should have a risk management program that allows [them] to identify, measure, monitor and control the risks related to social media."
- Legal risks: application of many laws and regulations to social media use
  - Truth in SavingsAct/Regulation DD and Part 707, Truth in Lending Act/Regulation Z
  - Equal Credit Opportunity Act, Fair Housing Act
  - Fair Debt Collection Practices Act
  - UDAP prohibition in Section 5 of the FTC Act, UDAAP prohibition in CFPB Act
  - Electronic Fund Transfer Act, Bank Secrecy Act, Community Reinvestment Act
  - Gramm-Leach-Bliley Act, the CAN-SPAM Act, TCPA, COPPA
- Reputational risks
  - on-line fraud and its possible effect on brand identity
  - reliance on third-party service providers and the need for adequate monitoring
  - transparency and privacy obligations in dealing with customers and clients
  - employee use of social media
- Operational risks: *cf.* FFIEC IT Exam Handbook
- Roughly 80 comments received
  - Overregulation, lack of flexibility in face of rapid technological evolution
  - Difficulties, costs of monitoring, influence third-party activity
  - Uncertain applicability, costs of possible disclosure obligations

Corporate Governance

- **SEC**
  - October 2011 Guidance
  - Continued issuance of inquiry letters
  - Rockefeller letters to Fortune 500, September 2012
  - Exchange between Chair White and Senator Rockefeller, April/May 2013

- **Management Oversight**
  - Board responsibility
  - CISO?
  - Audits and active planning
  - Don't wait for a major breach

Insurance

- **Market continues to grow** – commercial premiums over $1 billion/year – but still probably only 1/3 or so of U.S. public companies have cyber coverage

- **Fights in the courts** over whether various kinds of cyber-related losses are covered under more traditional policies are proliferating
  - *Hartford Casualty Insurance Co. v. Corcino & Assocs.*, (C.D. Cal. Oct. 7, 2013): exclusion for violations of statutory rights does not shield insurer for coverage of data breach involving medical information
  - *Retail Ventures, Inc. v. National Union Fire Insurance Co.*, 691 F.3d 821 (6th Cir. 2012): remediation costs in first-party losses under computer fraud rider; exclusion for "proprietary information" not triggered
- **In selecting cybersecurity insurance**, need to understand possible types of loss: not just first-party versus third-party, but elements
  - Replacement or restoration of data
  - Damage to physical property, such as computers
  - Business interruption losses
  - Costs of compliance with consumer notification laws
  - Costs of internal investigation and response
  - Remediation costs, such as credit monitoring for affected individuals
  - Response to government investigations
  - Regulatory penalties and fines
  - Judgments, settlements, and defense costs
  - Public relations expenses
  - Cyber-extortion

Big Data

- **Definitions**
  - Volume, Velocity, Variety
  - Some sources:
    - Social media
    - Behavioral tracking
    - Machine-generated
- **Growing market for enterprise technologies**
  - IDC: $3.2 to $16.9 billion from 2010 to 2015
- **Emerging Issues**
  - Indiscriminate collection/over collection; genuine consent
  - De-identification
  - Retention, destruction
  - Catastrophic breaches: water in a glass vs. water behind a dam
- **Increased Regulatory Interest**
  - FTC: Recent Brill, Vladeck speeches
  - Congressional data broker investigations

The FTC's New Rules Concerning Children's Privacy

Overview of the Children's Online Privacy Protection Act

- In its simplest application, COPPA requires that operators of commercial *websites* and *online services* that are *"directed to children"* must provide *notice* and obtain *parental consent* before *collecting* or *enabling disclosure* of "*personal information*" from a *child* online.
  - "Online service" is defined broadly. The law applies not just to websites, but also mobile apps, Internet-enabled gaming platforms, internet-enabled location-based services, etc.
  - There is a multi-factor test for whether a site or service is "directed to children."
    - A portion of a general-audience website can be directed to children (e.g., a "kids korner").
    - Even a general-audience service must comply with COPPA when it has "actual knowledge" that it has collected personal information from a child or from users of a "child directed" site or service.
  - The law requires two types of notice in most circumstances:
    - A COPPA-compliant online privacy policy that discloses certain info specified in the rules; and
    - A notice delivered directly to the child's parent before collecting any information about the child.

Overview of the Children's Online Privacy Protection Act

- In its simplest application, COPPA requires that operators of commercial *websites* and *online services* that are *"directed to children"* must provide *notice* and obtain *parental consent* before *collecting* or *enabling disclosure* of "*personal information*" from a *child* online.
  - In many circumstances, a site or service must get consent from the parent prior to collecting (or disclosing) information from a child. There are a number of exceptions to this requirement.
  - The law governs not just collection of information from children, but also any features that make it possible for children to disclose information about themselves (e.g., chat rooms, comment fields).
  - "Personal information" is defined extraordinarily broadly, and includes things that are not considered personally identifiable information in other contexts, such as IP addresses and cookies.
  - A "child" under COPPA is one under the age of 13.

The FTC's New COPPA Rules

- The Federal Trade Commission issued new rules interpreting COPPA that went into effect on July 1st.
- The new rules expand the definition of "personal information":
  - Prior to the amendments, "personal information" included: full name, physical address, online contact information, telephone number, social security number, and other information combined with personal information.
  - The FTC added four types of information to the definition:
    - Geolocation information sufficient to identify the street name and the name of the city/town; the FTC clarified that this information is covered by the ***existing*** rule
    - Photos, videos, or audio files that contain a child's image or voice
    - Screen or user names that function like "online contact information"
    - "Persistent identifiers" that can be used to recognize a user over time ***and*** across different sites or services (e.g., cookies, device IDs, IP addresses). [But note: When an operator collects a persistent identifier and no other personal information, there is no notice or consent requirement when the identifier "is used for the sole purpose of providing support for the internal operations of the Web site or online service."]

Third-Party Liability and the "Actual Knowledge" Standard

- A general-audience website or service must comply with COPPA when the operator has "actual knowledge" that it has collected personal information from a child (e.g., through a customer service interaction or a post on a monitored message board).
- A third-party plug-in, ad network, or other service that collects personal information through another site or service must comply with COPPA if it has "actual knowledge" that it is integrated into a child-directed site or service.
- Although a strict-liability standard applies for "child-directed sites," it does not apply to general-audience services and plug-ins. Instead, a third party has actual knowledge when:
  - The child-directed website or service directly communicates the nature of its content to the third-party provider; or
  - A representative of the third party recognizes the child-directed nature of the site.

Additional Features of the FTC's New Rules

- The new rules impose strict liability for child-directed websites and services. This element is controversial and garnered a dissent from Commissioner Ohlhausen.
- The new rules contain guidance and restrictions for third-party social media plug-ins (like Facebook share), ad networks, and analytics providers (like Google Analytics).
- Under the old rules, *all* child-directed sites were required to assume that all users were under 13 and provide appropriate COPPA protections. The new rules allow a subset of child-directed sites to age-screen users.
- The new rules permit the use of additional mechanisms for obtaining parental consent, such as video conferencing.
- The FTC altered (and in some ways streamlined) the privacy policy and parental notice requirements.
- The new rules strengthen existing security protections and add new obligations concerning data retention and deletion.

Thank You and Contact Information

Jonathan Cedarbaum
+1 202 663 6315
Jonathan.Cedarbaum@wilmerhale.com

Robert Finkel
+1 212 295 6555
Robert.Finkel@wilmerhale.com

Heather Zachary
+1 202 663 6794
Heather.Zachary@wilmerhale.com

WilmerHale has been accredited by the New York and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer 1.0 CLE credit in New York and California. Please note that no partial credit will be awarded. Attendees requesting CLE credit must attend the entire program.