FinTech Webinar Series:

CYBERSECURITY AND DATA PRIVACY

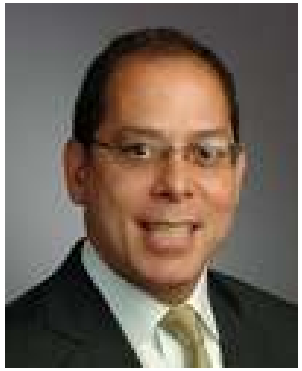
Jonathan Cedarbaum, Robert Finkel, and Heather Zachary

January 24, 2013

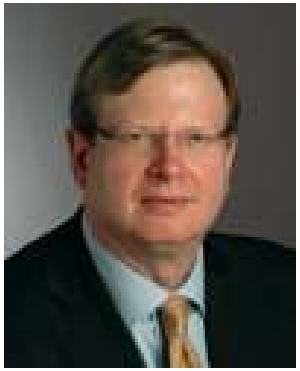
WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Speakers



Jonathan G. Cedarbaum
Partner
WilmerHale



Robert Finkel
Partner
WilmerHale

Heather Zachary
Partner
WilmerHale

Overview

1. Storage and Processing of Data in "the Cloud"
2. Mobile Devices and Mobile Apps
3. "Big Data"
4. Security and Privacy Issues in Third-Party Contracts
5. Data Security and Corporate Governance
6. International Privacy and Data Security
7. Data Security as a National Security Concern: Legislation and Executive Initiatives

Storage and Processing of Data in "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

Gramm-Leach-Bliley Act

- Physical, administrative, and technical safeguards to protect the security, confidentiality, and integrity of customer information and records, and to protect against unauthorized access to or use of such records or information
- Interagency Guidelines Establishing Information Security Standards (e.g., appendix to 12 CFR part 225) and FTC Safeguards Rule (16 CFR part 314)
  - Information security program
- Broad definition of "financial institution": engaged in "financial activities" at all, including lending, exchanging, transferring, investing for others, or safeguarding money or securities; insuring or indemnifying against loss; providing financial, investment, or economic advisory services; etc. (12 U.S.C. 1843(d)(4))

FFIEC and Bank Service Company Act

FFIEC

- IT Examination Handbook
  - Supervision of Technology Service Providers (Oct. 2012)
  - Outsourcing Technology Services
  - Information Security
- Statement on "Outsourced Cloud Computing" (July 10, 2012)
- Draft Guidance on Social Media (Jan. 23, 2013)

Bank Service Company Act, 12 U.S.C. § 1861 et seq.

Contracting Considerations

- Assessing Security Standards of Cloud Providers
  - NIST Security Control Recommendations
  - Cloud Security Alliance, Guidelines and Registry
- Some Typical Contract Clauses To Consider
  - Customer audits/access to logs
  - Data deletion
  - Downtime credits/indemnification
  - Encryption

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, 15 U.S.C. 6801 et seq., 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.

Mobile Devices and Mobile Apps

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 (2012), http://business.ftc.gov/sites/default/files/pdf/bus81-marketing-your-mobile-app.pdf
  - 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 government has recognized the promise of big data and is capitalizing on the technology itself.
  - The White House's Big Data Research and Development Initiative is using 84 different big data programs to address important problems facing government.
  - Massachusetts' Big Data Initiative provides funding to research institutions.

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 in the FinTech space.
- 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 FinTech Companies Leveraging Big Data

- FinTech companies are increasingly looking to leverage the data they have collected, but the legal landscape is complex and rapidly changing.
- A variety of federal laws apply to FinTech companies:
  - Gramm-Leach-Bliley Act
  - Fair Credit Reporting Act
  - Federal Trade Commission Act
  - The Wiretap Act and the Electronic Communications Privacy Act
- A multitude of state laws apply as well.
  - State analogues to the Gramm-Leach-Bliley Act and the FTC 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

Security and Privacy Issues in Third-Party Contracts

Security and Privacy Issues in Third Party Contracts

- Financial institutions historically have relied extensively on third-party vendors
- Reliance on Third-Party Outsourcing and Other Vendors May Increase
  - Pressure on financial institutions to reduce costs
  - Increased regulatory compliance burden
  - Technology software and service solutions to regulatory-related issues
- Third-Party Vendors will be asked to assume roles of increasing importance
  - As roles increase, so does the risk to the financial institution

Security and Privacy Issues in Third Party Contracts

- All regulatory guidance has a consistent theme: while functions may be outsourced, accountability remains with the institution and its Board of Directors
- Privacy, Confidentiality and Security Clauses now are heavily negotiated provisions
  - Parties spend much more time on these issues than in the past
- 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

Security and Privacy Issues in Third Party Contracts

- Some Contract Terms Takeaways:
  - Clear Delineation of Responsibility of Parties
  - Data Security Terms
    - Prompt Reporting and Remediation of Security Breaches or Attempted Breaches
    - Agree on Proper Materiality Threshold
    - Reporting on Every Attempt Simply not Feasible
- Vendor monitoring of legislative and regulatory changes
  - Sharing of best practices from other engagements
- Vendor commitment to modify software/services to comply with changes in law.

Data Security and Corporate Governance

SEC Disclosure Requirements

- On Oct. 13, 2011, Securities and Exchange Commission's Division of Corporation Finance issued guidance on disclosure obligations relating to cybersecurity risks and incidents.
- Notes several types of negative consequences public companies may confront in the wake of a cyber incident, including remediation costs, costs of increased cybersecurity protection measures, lost revenues, litigation costs, and reputational damage.
- In light of the damage a cyber incident can cause and existing obligations to disclose information that a "reasonable investor would consider important to an investment decision," companies may be required to provide information that allows investors to understand the nature of a company's cybersecurity risks.
- "Appropriate disclosures may include . . . description of relevant insurance coverage"
- Senator Rockefeller: The guidance "fundamentally changes the way companies will address cybersecurity in the 21st century."
- SEC sending out inquiry letters based on public statements, filings

Corporate Governance

- Cybersecurity as risk management
- Board involvement?
- CISO?
- External audit?
- Incident response planning and practice
- Insurance?

Incident Response

Key Issues To Prepare for in Advance:

- Planning for Multiple Incidents: Tailored procedures for handling different types of information security incidents
- Analytic Capacity: Analysis and identification of the cause of the incident
- Clear Documentation Requirements: Steps for gathering information and documenting incident
- Escalation of Serious Intrusions: Criteria for prioritizing incidents and assessing the criticality of the affected resources
- Mechanism to Mandate Corrective Action: Procedures for planning and implementation of corrective steps
- Communication Protocols: Procedures for communication with those affected by or involved with recovery from the incident
- Forensics: Collection and preservation of audit trails/other evidence

Insurance

- SEC Disclosure Guidance: "Appropriate disclosures may include … description of relevant insurance coverage"
- DHS Oct. 2012 Workshop and Readout Report
- "Insurance Against Cyber Attacks Expected To Boom," *New York Times*, Dec. 29, 2011: $750 million in premiums placed?
- 30-40 carriers in U.S.?
- Increasing litigation over scope of traditional and new policies
- ENISA, Incentives and Barriers of the Cyber-Insurance Market in Europe (June 5, 2012)

International Privacy and Data Security

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 month 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 in April, and a final agreement between the Parliament and the Council could occur by late 2013.

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 mandatory data breach reporting requirement.

Other International Developments Relevant to FinTech Companies

- Potential for increased enforcement of the EU "Cookie Directive." (Directive 2009/135/EC)
  - The extraterritorial reach of the Cookie Directive is extraordinarily expansive.
  - In some countries, certain types of cookies require affirmative, opt-in consent.
  - Many countries requires banner warnings or website overlays and clear notice to consumers regarding cookies.
  - Many U.S. companies are not yet in compliance with the directive.
- Continued implementation of APEC's Cross Border Privacy Rules.
- Implementation of additional rules in the United Kingdom regarding online behavioral advertising.

Data Security as a National Security Concern: Legislation and Executive Initiatives

Threats and Risks

- **Attack and Espionage**
  - **War/Terrorism**
  - **Private-sector targets, including financial sector:**
    Shamoon, 8/15/2012
    DDoS attacks on big U.S. banks: "Bro-bot" botnet, Sept. 2012; again in December 2012
  - **Hactivists**: Anonymous, Lulzsec

- **Theft of IP/Money**
  - 2012 Norton Cybercrime Report: $110 billion worldwide
  - 2012 Ponemon Cost of Cybercrime Study: average $8.9 million/breach
  - Project Blitzkrieg?

- **Disclosure/Theft of Personally Identifiable Information**
  - 2005-2011: >2,300 breaches; > 535 million records
  - Banks and payment services frequent targets because of financial information, e.g., June 2011: Citibank acknowledges intrusion stealing personal information of more than 200,000 customers
  - S.C. Dept. of Revenue, Sept. 2012: PII of 3.6 million taxpayers, including SSNs
  - Not always intrusions; sometimes more old-fashioned causes, e.g., theft/loss of media

Legislative Developments

Push for New Legislation in Fall 2011/Early 2012

- *Senator Reid Letter to Senator McConnell* (Nov. 2011):
  "Given the magnitude of the threat and the gaps in the government's ability to respond, we cannot afford to delay action on this critical legislation. For that reason, it is my intent to bring comprehensive cybersecurity legislation to the Senate floor for consideration for the first senate work period next year."
- Administration classified briefings
- House Republican cybersecurity task force
- But cautionary letter from Republican Senators, U.S. Chamber of Commerce

Legislative Developments

Senate Lead Omnibus Bill: S. 2105/S. 3414

- Introduced Feb. 14, 2012
- Principal co-sponsors: Lieberman (D-CT), Collins (R-ME), Rockefeller (D-WV), Feinstein (D-CA)
- Hearing Feb. 16 before Homeland Security and Government Affairs Committee
- Mixed reception
  - Oracle/Cisco, Tech America, NDIA
  - U.S. Chamber, many financial industry associations
- Failure to get cloture, Aug. 2012, 52-46; Nov. 14, 51-47

Legislative Developments

S. 2105/S. 3414 Key provisions:

- **Critical Infrastructure**: would authorize the Department of Homeland Security (DHS) to identify and establish cybersecurity performance standards for "covered critical infrastructure," such as important energy, financial, telecommunications, and transportation systems or assets (Title I); critical infrastructure includes:
  - **catastrophic economic damage** to the United States including:
    - **(a) failure or substantial disruption of a United States financial market**;
    - (b) incapacitation or sustained disruption of a transportation system; or
    - **(c) other systemic, long-term damage to the United States economy**
- **Information-sharing**: would clarify the authority of owners of information systems to monitor and undertake "countermeasures" on their own systems and would create institutions and legal incentives for the sharing of cyber threat and response information among businesses and between businesses and the federal government (Title VII);
- **FISMA reform/Federal networks**: would strengthen the ability of the federal government to protect its own networks and centralize enhanced authority in DHS (Titles II and III)
- No federal data breach notification title

Legislative Developments

"SECURE IT ACT" (McCain/Hutchison et al. Alternative):

S. 2151/ S. 3342

- Introduced March 1, 2012
- Sponsors: McCain (R-AZ), Hutchison (R-TX), Chambliss (R-GA), Grassley (R-IA), Murkowski (R-A), Coats (R-IN), Burr (R-NC), Johnson (R-WI)

Key Provisions:

- Information-Sharing
- FISMA Reform
- Criminal Penalties
  - New penalties for damaging critical infrastructure computers
  - Limits use of CFAA where exceeding authorized access based on service agreement
- No Critical Infrastructure Requirements or Federal Data Breach Notification Standards

Legislative Developments

"Cybersecurity Week" in the House (April 2012)
H.R. 3523, Cyber Intelligence Sharing and Protection Act ("CISPA")

- Would give qualified companies access to classified cyber threat data from NSA and other intelligence agencies to help protect their networks
- Would immunize companies and their cybersecurity providers from liability for good faith using, sharing of such information in aid of cybersecurity efforts
- Information disclosed to the Government, other companies could be used in accordance with restrictions established by sharing entity, not to gain competitive advantage; Government may not use it for a "regulatory purpose," but only for "cybersecurity purposes," including investigation of cyber crimes, to protect minors, national security, individuals in danger of death or injury
- Express preemption of contrary State laws
- House Intelligence Committee approved 17-1 on Dec. 1, 2011
- Substantial industry support: FS Roundtable; US Chamber; Tech America; USTelecomm;
- But controversy over lack of privacy protections, tighter restrictions on Government use of data
- Veto threat

Executive Order?

Draft Order deliberately leaked late September, early October; new version, November 21

Basic provisions:

- Commerce/NIST to develop consensus framework of voluntary cybersecurity performance standards;
- DHS Sec'y to coordinate identification of critical infrastructure; urge adoption of standards via sector-specific agencies; with Treasury, Commerce to recommend incentives possible under existing law for critical infrastructure owners and operators who comply
- Agencies with regulatory authority over critical infrastructure directed to determine whether they have "clear authority" to make standards mandatory
- DHS, DoJ, DNI directed to establish more effective system for sharing of government cyber threat information with critical infrastructure owners and operators;
- DoD and GSA to recommend government contracting preferences for companies that satisfy new cyber standards

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