PRIVACY AND DATA PROTECTION LEGISLATION: THE RISKS AND WHAT CORPORATE COUNSEL NEED TO KNOW

October 5, 2011

Presented by:

James R. Tucker, Jr.
(202) 887-4279
jtucker@akingump.com

Francine E. Friedman
(202) 887-4143
ffriedman@akingump.com

Jo-Ellyn Sakowitz Klein
(202) 887-4220
jsklein@akingump.com

Daniel F. McInnis
(202) 887-4359
dmcinnis@akingump.com

AKIN GUMP
STRAUSS HAUER & FELD LLP

TABLE OF CONTENTS

PRIVACY AND DATA PROTECTION LEGISLATION: THE RISKS AND WHAT CORPORATE COUNSEL NEED TO KNOW

October 5, 2011

Presented by:

James R. Tucker, Jr.
(202) 887-4279
jtucker@akingump.com

Francine E. Friedman
(202) 887-4143
ffriedman@akingump.com

Jo-Ellyn Sakowitz Klein
(202) 887-4220
jsklein@akingump.com

Daniel F. McInnis
(202) 887-4359
dmcinnis@akingump.com

AKIN GUMP
STRAUSS HAUER & FELD LLP

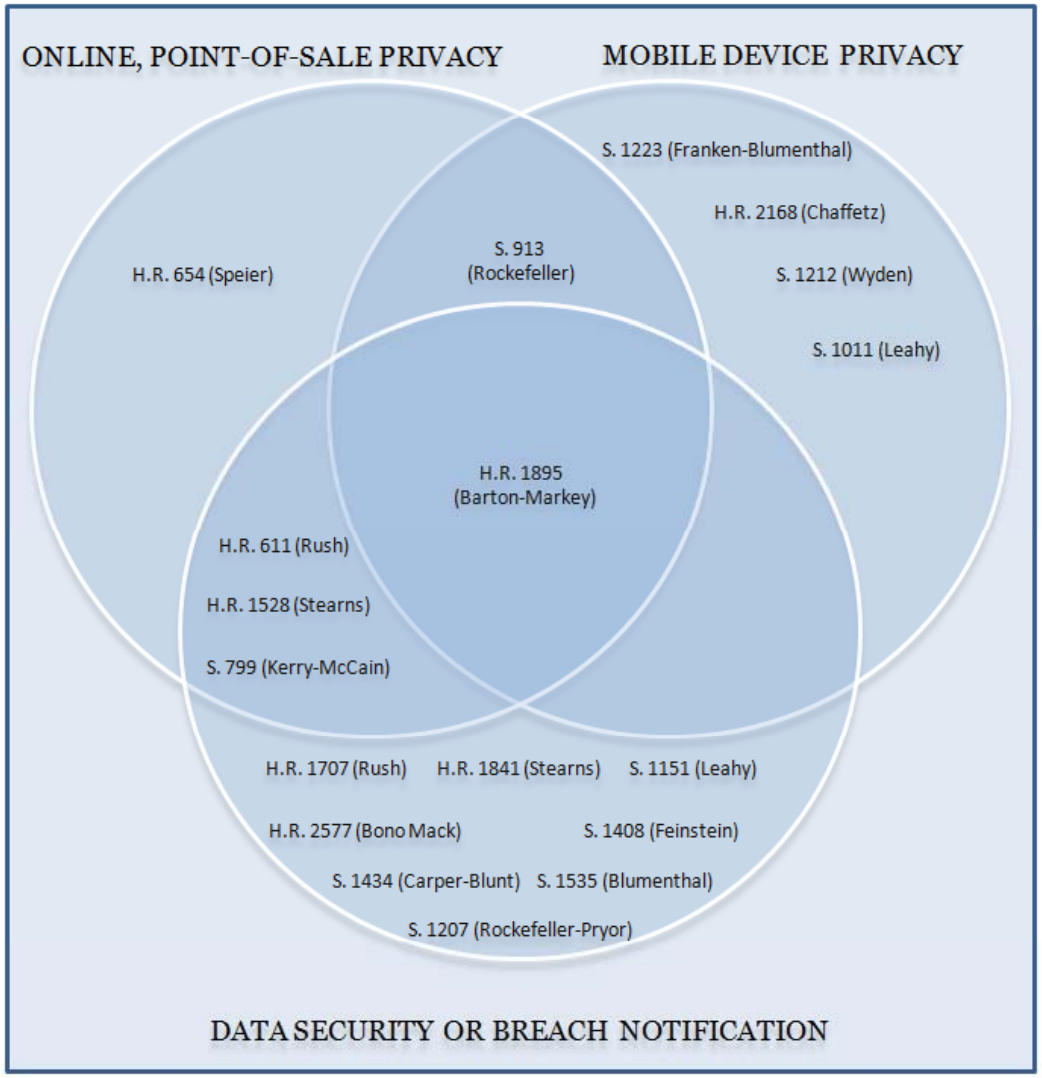
Privacy and Data Protection Legislation:
The Risks and What Corporate Counsel Need to Know

- Congressional Data Security and Privacy Proposals
- Recent Administration Activities Supporting Legislation
- Outlook for Legislative and Regulatory Proposals
- Lessons Learned From HIPAA and HITECH
- Recent FTC Privacy Enforcement and Implications
- Potential Impact on Businesses and Non-profit Organizations
- Steps to Take Now

Congressional Data Security and Privacy Proposals

- Constant stream of breaches has focused the public and media attention on consumer privacy and data security issues
- Lawmakers feel compelled to respond
- Very few issues have received bipartisan, bicameral attention in the 112th Congress, but privacy and data security are among them
  - 18 bills have been introduced - by members of both parties, in both chambers, some with bipartisan sponsorship
  - At least 17 hearings across four congressional committees in 2011
  - Dozens of town halls, policy roundtables, and stakeholder conversations

Legislative Proposals:
A Visual Guide



Legislative Proposals:
A Timeline

JANUARY

FEBRUARY
- H.R. 611 (Feb. 10)
- H.R. 654 (Feb. 11)

MARCH

APRIL
- Epsilon breach (April 2)
- S. 799 (April 12)
- H.R. 1528 (April 13)
- SSA breach (April 14)
- iPhone/Android tracking (Apr. 20)
- Sony breach (April 27)

MAY
- H.R. 1707 (May 4)
- S. 913 (May 9)
- H.R. 1841 (May 11)
- H.R. 1895 (May 13)
- S. 1011 (May 17)

JUNE
- S. 1151 (June 7)
- Citi breach (June 9)
- H.R. 2168/S. 1212 (June 15)
- S. 1207 (June 15)
- S. 1223 (June 16)

JULY
- H.R. 2577 (July 18)
- S. 1408 (July 22)
- S. 1434 (July 28)

AUGUST
- Congressional Recess

SEPTEMBER
- S. 1535 (Sep. 8)
- SAIC breach (Sep. 29)

Legislative Proposals:
Data Security, Breach Notification

- Sen. Feinstein (D-CA): *Data Breach Notification Act of 2011 (S. 1408)*
  - Creates new breach notification standards that would be triggered in breaches where there is risk of identity theft, economic loss, or harm to the affected individuals
  - Does not address data security
  - Recently reported out of the Judiciary Committee
- Sen. Leahy (D-VT): *Personal Data Privacy and Security Act (S. 1151)*
  - Sen. Leahy Chairs the Senate Judiciary Committee
  - Calls for businesses to enact security procedures to protect sensitive data
  - Creates new breach notification standards that would be triggered in cases where there is risk of identity theft, economic loss, or harm to the affected individuals
  - Recently reported out of the Judiciary Committee
- Sen. Blumenthal (D-CT): *Personal Data Protection and Breach Accountability Act of 2011 (S. 1535)*
  - Requires new safeguards for stored information and puts in place new breach notification, breach remedy, and breach investigation standards
  - Recently reported out of the Judiciary Committee

Legislative Proposals:
Data Security, Breach Notification

- Sens. Rockefeller (D-WV) and Pryor (D-AR): *Data Security and Breach Notification Act of 2011 (S. 1207)*
  - Senator Rockefeller Chairs the Commerce Committee
  - Requires businesses and non-profit organizations to implement security measures and alert consumers when data has been compromised
  - In the event of a breach, affected individuals would be entitled to free credit monitoring services for two years
  - This bill broadens the definition of covered entities to go beyond businesses, specifically singling out non-profit organizations

- Sens. Carper (D-DE) and Blunt (R-MO): *Data Security Act of 2011 (S. 1434)*
  - Requires entities that possess sensitive information to build safeguards
  - Enact policies for investigating security breaches and notifying consumers when a substantial risk of identity theft or account fraud exists

Legislative Proposals:
Data Security, Breach Notification

- Rep. Bono Mack (R-FL): *SAFE Data Act (H.R. 2577)*
  - Rep. Bono Mack Chairs the Commerce, Manufacturing, and Trade Subcommittee of the House Energy & Commerce Committee
  - Requires notification of consumers and the FTC after a breach is contained and assessed
  - Calls for stronger data security systems
  - Entitles affected individuals to free credit monitoring services for two years

- Rep. Stearns (R-FL): *DATA Act of 2011 (H.R. 1841)*
  - Requires tighter protections of data storage
  - Creates a standard for notifying affected individuals and government authorities in the event of a breach

- Rep. Rush (D-IL): *Data Accountability and Trust Act (H.R. 1707)*
  - Mandates stricter data security policies and creates a national standard for breach notification

Legislative Proposals:
Privacy

- Sen. Rockefeller (D-WV): *Do-Not-Track Online Act of 2011 (S. 913)*
  - Gives consumers the ability to opt out of having their online data tracked and stored
  - Goes one step further than other privacy bills by also imposing limits on data collection from mobile devices

- Sens. Kerry (D-MA) and McCain (R-AZ): *Commercial Privacy Bill of Rights Act of 2011 (S. 799)*
  - Requires opt-out mechanisms for data sharing, as well as opt-in consent for the collection, storage, or sharing of sensitive personal information

Legislative Proposals: *Privacy*

- Reps. Markey (D-MA) and Barton (R-TX): *Do-Not-Track-Kids Act (H.R. 1895)*
  - Markey and Barton are Co-Chairs of the Bipartisan Congressional Privacy Caucus
  - Forbids online companies from using personal information for targeted marketing to children under the age of 18
  - Empowers parents to delete their children's digital footprint, and requires parental consent for any data tracking online or on mobile devices
- Rep. Speier (D-CA): *Do Not Track Me Online Act of 2011 (H.R. 654)*
  - Requires opt-out mechanisms for the collection or use of online and personal data
- Rep. Rush (D-IL): *BEST PRACTICES Act (H.R. 611)*
  - Requires opt-out mechanisms for data collection and storage, as well as opt-in consent for third party information sharing
- Rep. Stearns (R-FL): *Consumer Privacy Protection Act of 2011 (H.R. 1528)*
  - Allows consumers to opt out of having their personally identifiable information shared with third parties
  - This bill broadens the definition of covered entities and specifically singles out 501(c)(3) organizations as covered, in addition to businesses

Legislative Proposals:
Mobile Device Privacy

- Sen. Wyden (D-OR) and Rep. Chaffetz (R-UT): *Geolocation and Privacy Surveillance (GPS) Act (S. 1212, H.R. 2168)*
  - Released as companion bills in the Senate and House
  - Prohibit companies from collecting or sharing geolocation information without the user's express consent
- Sens. Franken (D-MN) and Blumenthal (D-CT): *Location Privacy Protection Act of 2011 (S. 1223)*
  - Requires any covered entity to offer upfront notice and receive informed consent from users to track their geolocation information
- Sen. Leahy (D-VT): *Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011)*
  - Enacted in 1986, the ECPA restricts third-party access to private electronic communications, such as online activity and e-mails
  - Leahy's proposal adds geolocation information as a new class of private communications subject to the protections of the ECPA
- Other bills in the works?
  - Recent Senate letter to OnStar, criticizing its geolocation tracking policies

Legislative Proposals:
Interplay With Current Law

- Will existing FEDERAL statutes retain jurisdiction where overlap occurs with new privacy legislation? Under most proposals, yes.
  - Family Educational Rights and Privacy Act (FERPA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Gramm-Leach-Bliley Act (GLBA)
  - Fair Credit Reporting Act (FCRA)
  - Health Information Technology for Economic and Clinical Health Act (HITECH)

- Will existing STATE statutes retain jurisdiction where overlap occurs with new privacy legislation? Under most proposals, no.
  - Replacing the patchwork of state laws with a single national standard

Privacy and Data Protection Legislation:
The Risks and What Corporate Counsel Need to Know

- Congressional Data Security and Privacy Proposals
- Recent Administration Activities Supporting Legislation
- Outlook for Legislative and Regulatory Proposals
- Lessons Learned From HIPAA and HITECH
- Recent FTC Privacy Enforcement and Implications
- Potential Impact on Businesses and Non-profit Organizations
- Steps to Take Now

Recent Administration Activities:
Overview

- The Obama Administration is actively engaged in the privacy debate
  - Federal Trade Commission
  - Department of Commerce
  - Interagency Subcommittee on Privacy and Internet Policy
    - 12 departments and agencies participating
    - Goal is to foster consensus in legislative, regulatory, and international internet policy
- Even if Congress fails to act, the Administration and FTC Will Seek to Expand Privacy Obligations

FTC Privacy Policy Debate & Legislative Focus

- FTC support for current legislative activity
  - FTC highly legislatively focused
- December 2010 Interim Staff Report:
  - "*Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*"
  - Three Part Focus: (1) Privacy by Design, (2) Choice, (3) Notice & Access
  - Modeled upon fair information practices
  - Controversial "do not track" proposal
  - Huge number of open issues and questions
- Strong "dissents"/concurrences by Republican commissioners
- Nine FTC appearances before Congress supporting legislation
  - Continued "dissents" by Commissioners Rosch & Kovacic
- Final FTC Staff Report expected late this year

Book-Ends of the FTC Policy Debate

- Comprehensive Reform vs. Learn More
  - Do we want to be more like Europe?
  - Changing technology
    - Rosch has suggested a 6(b) Industry wide study
- FIP vs. Harm-Based
  - Doubts about notice and choice
  - Opt-in/opt-out controversy
  - Benefits of “access”
  - Legal mandate vs. self-regulation
- Do Not Track
  - Practical?
  - Do Not Call precedent
  - Industry efforts to meet actual consumer demand for privacy protection

The FTC of the Future:
How Might the FTC Change Under Proposed Legislation?

- New Powers
  - APA Rule-Making, Civil Penalties, Federal Court Litigation
- New Substance
  - FTC may, in consultation with the Attorney General, issue regulations as it determines necessary to carry out the security breach notification provisions
  - FTC may treat any data security mandate or breach notification violation as an unfair and deceptive trade practice
  - FTC would be required to develop standards for a "Do Not Track" mechanism
  - FTC would be able to promulgate rules (after conducting a study) to require standard destruction methods for paper and non-electronic data
  - FTC would be required to promulgate rules requiring covered entities to enact security measures, provide privacy notices, and obtain opt-in consent for certain disclosures to third parties.

Department of Commerce

- December 2010: Internet Policy Task Force green paper, "Commercial Data and Privacy Innovation in the Internet Economy: A Dynamic Policy Framework"
  - Started the conversation, solicited feedback to inform the final report
  - Final report expected in the near term (Democrats in Congress have called on Commerce to act quickly)

- June 2011: Internet Policy Task Force report, "Cybersecurity, Innovation, and the Internet Economy"
  - National standard to minimize data security vulnerabilities on the internet
  - National data breach notification standard
  - Stricter penalties to combat data security threats
  - Increased data security education and research
  - International coordination to create a common standard and share best practices

Privacy and Data Protection Legislation:
The Risks and What Corporate Counsel Need to Know

- Congressional Data Security and Privacy Proposals
- Recent Administration Activities Supporting Legislation
- Outlook for Legislative and Regulatory Proposals
- Lessons Learned From HIPAA and HITECH
- Recent FTC Privacy Enforcement and Implications
- Potential Impact on Businesses and Non-profit Organizations
- Steps to Take Now

Prospects for Legislative Action:
Reasons to Expect Stalemate

- Too many cooks in the kitchen?
  - Multiple Senate and House committees jockeying for jurisdiction
    - Senate Judiciary Committee (Leahy)
      - Subcommittee on Privacy, Technology, and the Law (Franken)
    - Senate Commerce Committee (Rockefeller)
      - Subcommittee on Consumer Protection, Product Safety, and Insurance (Pryor)
      - Subcommittee on Communications, Technology, and the Internet (Kerry)
    - House Judiciary Committee (Lamar Smith)
    - House Energy & Commerce Committee (Upton)
      - Subcommittee on Commerce, Manufacturing, and Trade (Bono Mack)
  - 18 bills introduced, and more likely to come

- Congressional paralysis in general

Prospects for Legislative Action:
Reasons to Expect Compromise

- Bipartisan and bicameral support exists for new privacy regulations
  - Data security and breach notification as potential areas for compromise
  - Industry leaders open to a federal data security and/or breach notification statute
    - Many would prefer a (reasonable) national standard to a patchwork of state laws
- Mutual signals between Congress and the Administration that action is needed
- Pressure from consumer groups
- How many more high-profile breaches before tipping point is reached?

Privacy and Data Protection Legislation:
The Risks and What Corporate Counsel Need to Know

- Congressional Data Security and Privacy Proposals
- Recent Administration Activities Supporting Legislation
- Outlook for Legislative and Regulatory Proposals
- Lessons Learned From HIPAA and HITECH
- Recent FTC Privacy Enforcement and Implications
- Potential Impact on Businesses and Non-profit Organizations
- Steps to Take Now

When Regulation Happens:
Tales from the Health Sector

- HIPAA and its implementing regulations create a complex federal scheme that protects the privacy and security of health information, layered atop more stringent state laws
- Enacted in 1996, HIPAA was implemented through primary rulemakings generally taking effect in 2003 (privacy) and 2005 (security)
  - Early focus on voluntary compliance and education
  - Initially enforcement strategy largely complaint-driven
- Changes to the HIPAA regime under the HITECH Act in 2009 dramatically enhanced risks relating to privacy and security
  - Extended reach to more entities
  - Increased penalties
  - New enforcement mechanisms
  - New audits
  - Breach notification requirements
- New Era of Enforcement

HIPAA Core Concepts:
Who Needs to Comply?

- Covered Entities
  - Health plans, health care clearinghouses, and certain health care providers are HIPAA covered entities
- Business Associates
  - HIPAA business associates provide services for or on behalf of covered entities, which involve PHI
  - Includes many software vendors and others in the technology space
  - Must enter into a “business associate agreement”
- New under HITECH: Business Associates Treated as Covered Entities
  - In addition to contractual liability, business associates now also face direct liability to regulators for penalties if they fail to comply with HIPAA privacy and security requirements

HIPAA Core Concepts:
What Information is Covered?

- HIPAA Protected Health Information
  - The HIPAA regulations generally apply to protected health information ("PHI"), which includes any information, whether oral or written, that is:
  - Created or received by a health care provider, health plan, employer, or health care clearing house;
  - Relates to the past, present, or future physical or mental health or condition of an individual, the provision of care to an individual, or the past present or future payment for the provision of health care to an individual; and
  - Identifies the individual (or could reasonably be expected to be used to identify the individual)

HIPAA Privacy Rule

- Core tenet of the HIPAA Privacy Rule
  - Do not use or disclose PHI without authorization, unless you are expressly permitted or required to do so
  - Examples of permitted uses and disclosures: treatment, payment, and healthcare operations ("TPO")
  - Examples of required uses and disclosures: required by law, pursuant to a court order
- Other key concepts
  - Minimum necessary
  - Individual rights

HIPAA Security Rule

- Core Goals of the HIPAA Security Rule
  - Ensure the confidentiality, integrity, and availability of electronic PHI ("ePHI") created, received, maintained, or transmitted by covered entities
  - Protect against reasonably anticipated threats and hazards to the security or integrity of ePHI
  - Protect against reasonably anticipated HIPAA privacy rule violations
- Basic Foundation for Compliance
  - Assessment and management of risk
  - Reasonable and appropriate policies and procedures
- HIPAA Standards and Implementation Specifications
  - Addressable (A) versus Required (R)
  - Not a one-size-fits-all approach
- Administrative, Physical and Technical Safeguards

HITECH Breach Notification Rule

- The HITECH Act created a new federal breach notification requirement
  - HHS Rule: HIPAA Covered Entities and their Business Associates
  - FTC Rule: Vendors of PHRs and certain PHR related entities (FTC)
- Establishes an expansive protocol for providing notice when an individual's “unsecured” PHI has been breached
- Depending on the circumstances, breach notification must be provided to individuals, HHS, and/or the media

HHS Breach Notification Rule:
"Wall of Shame"

U.S. Department of Health & Human Services

HHS.gov *Improving the health, safety, and well-being of America*

Search | Search OCR All HHS

HHS Home | HHS News | About HHS | Font Size | Print | Download Reader

Health Information Privacy

Office for Civil Rights | Civil Rights | Health Information Privacy

OCR Home > Health Information Privacy > HIPAA Administrative Simplification Statute and Rules > Breach Notification Rule

HIPAA
- Understanding HIPAA Privacy
- HIPAA Administrative Simplification Statute and Rules
  - Statute
  - Privacy Rule
  - Security Rule
  - Breach Notification Rule
  - Other Administrative Simplification Rules
  - Enforcement Rule
  - Combined Text of All Rules
- Enforcement Activities & Results
- How to File a Complaint
- News Archive
- Frequently Asked Questions

PSQIA
- Understanding PSQIA Confidentiality
- PSQIA Statute & Rule
- Enforcement Activities & Results
- How to File a Complaint

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Full DataSet CSV format (18 KB) XML format (57 KB)

Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.

Filter: 330 records showing

Name of Covered Entity	State	Individuals Affected	Date of Breach	Type of Breach	Location of Breached Info
Accendo	AZ	175,350	2011-01-01	Unauthorized Access/Disclosure	Paper
Advanced NeuroSpinal Care	CA	3,500	2009-12-30	Theft, Loss	Network Server, Computer
Advocate Health Care	IL	812	2009-11-24	Theft	Laptop
Aetna	CT	6,372	2010-03-29	Unauthorized Access/Disclosure	Paper
Aetna, Inc.	CT	2,345	2010-09-09	Unauthorized Access/Disclosure	Network Server
Affinity Health Plan, Inc.	NY	344,579	2009-11-24	Other	Other
Aiken Community Based Outpatient Clinic	SC	2,717	2011-02-16	Improper Disposal	Paper
Alaska Department of Health and Social Services	AS	501	2009-10-12	Theft	Portable Electronic Device

Name Of Covered Entity Accendo

State AZ

HIPAA and HITECH:
Penalties

- Enhanced penalties apply to covered entities (and business associates)
  - Civil penalties – $100 to $50,000 for individual violations based on level of intent or neglect; annual maximum of $1.5 million for violations of an identical provision
    - Unknowing violation – $100 to $50,000 per violation
    - Reasonable cause – $1,000 to $50,000 per violation
    - Willful neglect – if corrected, $10,000 to $50,000 per violation
    - Willful neglect – if not corrected, $50,000 per violation
  - Criminal penalties – up to $50,000 and a year in prison; the statute specifies this can apply to individuals as well as entities
    - Penalty increases to $100,000 and up to 5 years in prison if the wrongful conduct involves false pretenses
    - Penalty increases to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm

HIPAA and HITECH:
Penalties

- All money that the Office for Civil Rights (OCR) receives from settlements and penalties goes straight to OCR's coffers
  - Funds HIPAA and HITECH enforcement, education, and other actions

- Language from HITECH SEC. 13410(c):

  (1) IN GENERAL—Subject to the regulation promulgated pursuant to paragraph (3), any civil monetary penalty or monetary settlement collected with respect to an offense punishable under this subtitle or section 1176 of the Social Security Act (42 U.S.C. 1320d–5) insofar as such section relates to privacy or security shall be transferred to the Office for Civil Rights of the Department of Health and Human Services to be used for purposes of enforcing the provisions of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this Act.

HIPAA and HITECH:
Federal Enforcement Actions

- Providence Health & Services (2008) ($100,000 settlement)
- CVS (2009) ($2.25M settlement)
- Rite Aid (2010) ($1M settlement)
- Management Services Organization (2010) ($35,000 settlement)
- Cignet Health (2011) ($4.3M penalty)
- Massachusetts General Hospital (2011) ($1M settlement)
- UCLA Health System (2011) ($865,000 settlement)

Case Study:
Massachusetts General Hospital Enforcement Action

- In February 2011, Massachusetts General Hospital ("MGH") entered into a Resolution Agreement with HHS requiring it to pay $1 million to settle potential HIPAA privacy rule violations

- The agreement stemmed from the loss of PHI of 192 patients of an MGH infectious disease outpatient practice
  - The breach occurred when an employee inadvertently left documents containing patient schedules and billing forms on a subway train while commuting to work
  - The documents contained sensitive information, including names, dates of birth, medical record numbers, diagnoses, and health insurance data
  - HIV/AIDS patients were among those affected by the breach

Case Study:
Massachusetts General Hospital Enforcement Action

- OCR's subsequent investigation revealed that MGH failed to implement reasonable and appropriate safeguards

- In addition to the $1 million payment amount, the Resolution Agreement included a CAP requiring the hospital to:
  - develop and implement policies and procedures on physical removal and transport of PHI, laptop encryption, and USB drive encryption
  - train employees on these policies, and
  - specially designate an internal monitor to conduct assessments of MGH's compliance with the CAP semi-annually for a 3-year period

State Attorney General Actions Under HITECH

- Connecticut was the first state to use HITECH authority to enforce HIPAA
  - Connecticut's Attorney General sued insurer Health Net where unencrypted data containing financial information and medical records of nearly half a million of Connecticut enrollees was breached
  - Health Net also failed to provide timely notification of the breach, waiting over five months before alerting insurance commissioners
  - Health Net settled the case, paying $250,000 to Connecticut in damages and a contingent $500,000 payment if it is established that the breached information was used illegally and impacted plan members
- Vermont's Attorney General initiated the second HIPAA enforcement action of its kind, also against Health Net
  - Vermont's complaint arose out of the same breach as the Connecticut case, in which information on 525 Vermont residents were also lost
  - The complaint alleged violations of HIPAA, Vermont's Security Breach Notice Act, and the Consumer Fraud Act
  - Health Net ultimately agreed to a settlement with Vermont for $55,000 for the breach

HITECH Audit Program

- Historically, OCR has investigated potential violations of the HIPAA privacy and security rules based on the receipt of complaints or media reports
- Under the HITECH Act, HHS is required to conduct periodic audits of covered entities and business associates to ensure compliance with HIPAA rules
- In June 2011, HHS awarded two major contracts related to conducting HITECH audits pursuant to this statutory requirement
  - Booz Allen Hamilton was awarded a $180,000 contract for "audit candidate identification"
  - KPMG was awarded a $9.2 million contract to develop an audit protocol and conduct privacy and security audits with OCR supervision

Burden of Compliance

- Determine covered entity/business associate status
- Develop and update written policies and procedures
  - Policies and procedures need to be tailored to your organization
  - Policies and procedures should be reevaluated on a regular basis, as well as when specific incidents arise
- Ensure compliance in practice
  - Confirm full compliance with your own policies and procedures through thoughtful internal monitoring and audits
  - Engage in workforce training and revisit sanction policies
- Develop game plans
  - Prepare for state and federal investigations, data breaches, and audits

Privacy and Data Protection Legislation:
The Risks and What Corporate Counsel Need to Know

- Congressional Data Security and Privacy Proposals
- Recent Administration Activities Supporting Legislation
- Outlook for Legislative and Regulatory Proposals
- Lessons Learned From HIPAA and HITECH
- **Recent FTC Privacy Enforcement and Implications**
- Potential Impact on Businesses and Non-profit Organizations
- Steps to Take Now

FTC Enforcement Focus

- Privacy promises
- Data security
- Specific statutory or trade regulation rule cases
  - COPPA as example
- What we are not seeing
  - No bread-and-butter cases: big data breaches and retailers
  - No identity thieves cases
  - No brick and mortar
  - No non-profits/colleges and universities/government

Notable Privacy Promise Cases

- Twitter (final order)
  - Very lax internal password and email security allowed hackers to twice gain “administrative control” of service and send unauthorized messages
  - Promise to provide reasonable and appropriate security
  - GLB-like Safeguards requirements
- Borders bankruptcy (letter to court from bureau director)
  - Bankruptcy court overseeing liquidation – Privacy Ombudsman
  - Sale of PII to Barnes & Noble possible contrary to privacy policies?
    - Blocked and then approved this week with 15 day opt-out
  - Danger of inflexible privacy promises over time
- Google Buzz
  - Heavily criticized roll-out of social network service, Google Buzz
  - Basic issue violation of statements on use of Google customer PII
  - Precedent setting in:
    - First case in which GLB-like relief imposed without a data breach
    - First case in which substantive violation of US-EU Safe Harbor Framework alleged

Notable Data Security Cases

- SettlementOne Credit (and two related matters)
  - Creditor report consolidator whose customers were hacked and credit report information stolen
  - Must be read in light of FCRA, GLB, and Safeguards Rule overview
  - No civil penalties this time (Chairman Leibowitz and Commissioner Brill)
- Ceridian
  - Third-party services provider for businesses and employee information.
    - Payroll and back office – sensitive PII
  - Around 28,000 employee records hacked & accessed via SQL attack
    - Alleged most basic precautions not taken for well know & previously challenged vulnerabilities
- Lookout Services
  - Lookout provides immigration/citizenship verification support
  - 37,000 consumer files accessed by Lookout employee without authorization; not clear why
    - Lookout disclosed through breach notification letters

Statutory Example: *COPPA*

- COPPA rule review
  - Seeking comment on proposed changes to Children's Online Privacy Protection Rule to adapt to rapidly changing technology
    - Broader definition of PI but exempt interactive communities
    - More flexibility for parental consent
    - Safeguards for vendors, limited retention, and appropriate deletion
    - Audits for safe harbor participants
- Broken Thumbs Apps
  - First Mobile Apps settlement—online gaming and social network
  - $50,000 civil penalty
- Playdom
  - Online virtual world operator
  - Alleged to have collected and disclosed PII of children under 13 without parental consent
  - $3 million civil penalty—largest COPPA fine to date

Privacy and Data Protection Legislation:
*The Risks and What Corporate Counsel Need to K*now

- Congressional Data Security and Privacy Proposals
- Recent Administration Activities Supporting Legislation
- Outlook for Legislative and Regulatory Proposals
- Lessons Learned From HIPAA and HITECH
- Recent FTC Privacy Enforcement and Implications
- Potential Impact on Businesses and Non-profit Organizations
- Steps to Take Now

Potential Implications:
What Will New Regulations Mean For Your Organization?

- Litigation and Financial Liability
  - Authority to bring a civil action
  - Authority to bring a private right of action
  - Free credit monitoring or credit scores to affected individuals in the event of a breach
- Compliance Costs, Headaches
  - Prohibitions against sharing information with non-affiliate third parties
  - Limits to duration of maintaining personal information
  - Overhauling IT networks to “build in” data security measures rather than layering on new patches
  - Periodic risk assessments and employee/volunteer training
- Reputation
  - Requirements to notify law enforcement, affected individuals, service providers, business partners, and the media in case of a breach

Privacy and Data Protection Legislation:
The Risks and What Corporate Counsel Need to Know

- Congressional Data Security and Privacy Proposals
- Recent Administration Activities Supporting Legislation
- Outlook for Legislative and Regulatory Proposals
- Lessons Learned From HIPAA and HITECH
- Recent FTC Privacy Enforcement and Implications
- Potential Impact on Businesses and Non-profit Organizations
- Steps to Take Now

Next Steps:
What Should Corporate Counsel Do Right Now?

- Know your flows, and know which existing privacy and data protection laws apply to your business
- Confirm your privacy policies and procedures are written, understandable, and current
  - Evaluate policies and procedures vis-à-vis existing law and industry best practices
    - If your organization does not meet the standards already in place, adjusting to meet new regulations will be that much more difficult
  - Evaluate your policies and procedures vis-à-vis risks specific to your organization
- Assess operational compliance with written policies and procedures
- Assign one person (or a designated team) responsibility over privacy and security concerns
- Train your workforce on privacy matters and ensure that all employees understand the importance of data security and privacy
- Looking ahead, it is important to monitor the policy debate in Washington and to understand how proposals can impact your organization

PRIVACY AND DATA PROTECTION LEGISLATION: THE RISKS AND WHAT CORPORATE COUNSEL NEED TO KNOW

October 5, 2011

Presented by:

James R. Tucker, Jr.
(202) 887-4279
jtucker@akingump.com

Francine E. Friedman
(202) 887-4143
ffriedman@akingump.com

Jo-Ellyn Sakowitz Klein
(202) 887-4220
jsklein@akingump.com

Daniel F. McInnis
(202) 887-4359
dmcinnis@akingump.com

AKIN GUMP
STRAUSS HAUER & FELD LLP

SPEAKER BIOGRAPHIES

FRANCINE E. FRIEDMAN, Senior Policy Counsel
ffriedman@akingump.com

Washington, D.C. **T** +1 202.887.4143 **F** +1 202.887.4288

Practice Areas:
Public Law and Policy
Policy and Regulation
Tax
Privacy and Data Protection

Bar Admissions
District of Columbia
Maryland
Virginia

Education
J.D. College of William and Mary School of Law, 1999
B.A. Georgetown University, 1995

Francine Friedman brings a decade of government affairs and lobbying experience to the firm. She advises clients on a variety of issues including tax policy, involving housing, energy and new markets tax credits; financial services reform; data security; and energy issues.

Prior to joining Akin Gump, Ms. Friedman was senior vice president of Parven Pomper Strategies (PPS) Inc. and served as counsel in the government relations group at a global law firm.

In 2005, she was an instrumental part in the establishment of the GO Zone housing tax credits after Hurricane Katrina. She has worked with the IRS and Congress to encourage common-sense solutions to regulatory roadblocks impacting rebuilding in the Gulf States. Ms. Friedman has also led efforts to educate Congress on the appropriate point of regulation of natural gas liquids under a cap and trade regime. She has represented numerous client groups and coalitions on a variety of tax credit and tax preference issues with a focus on Section 29 and 45 (energy) and Section 42 (low-income housing) tax credits.

Ms. Friedman began her experience on Capitol Hill as an intern at the Democratic Senate Campaign Committee, working for then-Chairman Sen. John Breaux, D-La. She later played a key role in opening Sen. Dianne Feinstein's national fundraising office for her 1992 senate race, the first senatorial campaign in which the challenger raised more money than the incumbent.

Ms. Friedman serves on the board of directors of the National Kidney Foundation for the National Capital Area, the Washington Area Lawyers for the Arts and the Capitol Area Reach Program. She has served as pro bono outside general counsel to the Capitol Area Reach Program, and in 2005 was named St. Luke's House Volunteer of the Year. In 2006, Ms. Friedman was named one of the "Greater Washington Legal Elite" by *Washington SmartCEO*

magazine. She hosted a legal talk show broadcast on several Washington, D.C. radio stations from 2000 through 2009. From 2002 until 2007, she served as a monthly panelist on "Metrotalk," a local public interest talk show.

Ms. Friedman received her B.A. in government in 1995 from Georgetown University and her J.D. from William & Mary Law School in 1999. She is admitted to practice in Virginia, Maryland and the District of Columbia.

JO-ELLYN SAKOWITZ KLEIN, Senior Counsel
jsklein@akingump.com

Washington, D.C. **T** +1 202.887.4220 **F** +1 202.887.4288

Practice Areas: **Policy and Regulation**
Health Industry
Privacy and Data Protection

Bar Admissions
District of Columbia
Virginia

Education
J.D. Georgetown University Law Center, 1998
A.B. Duke University, 1994

Jo-Ellyn Sakowitz Klein devotes much of her practice to regulatory, transactional and legislative matters affecting the health industry. She also advises clients outside the health care sector that are affected by health care or privacy law and regulation.

Ms. Klein leads the firm's interdisciplinary privacy and data protection initiative. She devotes a substantial portion of her practice to assisting clients from across the spectrum with issues arising under state, federal and international privacy, security and data breach notification laws and regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the American Recovery and Reinvestment Act of 2009 (ARRA), the FTC Red Flags Rule adopted under the Fair and Accurate Credit Transactions Act (FACTA) of 2003, and the Genetic Information Nondiscrimination Act (GINA). She has examined privacy and security issues arising in settings ranging from hospitals to pharmacy chains to clinical research to professional sports.

Representative engagements in this area include—

- assisting clients with regulatory compliance questions arising in the course of their day-to-day operations—under the federal HIPAA and GINA regulations as well as under state privacy provisions
- evaluating whether contemplated marketing activities comply with federal and state privacy laws
- tailoring software license agreements and related transactional documents to address privacy issues
- drafting and negotiating targeted business associate agreements that meet the individualized needs of clients—whether they are covered entities, business associates, or downstream agents or subcontractors

- assisting clients facing allegations raised by individuals in HIPAA complaints filed with federal regulators

- helping clients prepare for and respond to data breaches, including evaluating whether notice of data breach requirements have been triggered and drafting appropriate breach notification correspondence

- addressing health information privacy issues arising in the course of litigation and in bankruptcy proceedings

- working with clients to identify risks relating to potential FTC enforcement activity, including evaluating whether an entity needs to comply with the FTC's Red Flags Rule.

Ms. Klein is a frequent speaker on topics relating to the health industry and data privacy issues. Recent speaking engagements include—

- "From the FTC to HHS: Making Sense of Recent Enforcement Activity," IAPP Washington DC KnowledgeNet (September 27, 2011)

- "Facebook and Twitter: Legal Liabilities and HIPAA Compliance in Healthcare," Progressive Healthcare Conferences (February 23, 2011)

- "HIPAA Compliance in a HITECH Age," National Constitution Conferences CLE webcast (October 6, 2010)

- "Comprehensive Privacy Legislation: Implications and Concerns for Business and Institutions," West LegalEdcenter webcast (July 22, 2010)

- "Facebook and Health Care Providers: Reaping the Benefits, While Managing the Risks," Progressive Healthcare Conferences (March 25, 2010)

- "New Red Flag Rules for Healthcare Providers: Are You Ready?" Panel convened by Strafford Publications (June 24, 2009 and October 7, 2009)

- "Social Networking and Healthcare Providers: Understanding the Risks," Webinar convened by Strafford Publications (October 22, 2009)

- "From HIPAA to ARRA and Beyond: Making Sense of Health Information Privacy and Security Requirements for Community Health Centers," Texas Association of Community Health Centers' 26th Annual Conference, Dallas (November 2, 2009)

Ms. Klein also assists clients, such as hospital systems, health plans and pharmaceutical companies, with regulatory and policy issues arising under the Medicare and Medicaid programs. She has focused on issues concerning Medicaid programs across the nation.

Ms. Klein received her A.B. in public policy studies and a certificate in education from Duke University in 1994. Prior to entering law school, she worked as a policy analyst at the University of California, Office of the President. She received her J.D. in 1998 from the Georgetown University Law Center, where she was an articles editor of *The Georgetown Law Journal*. Ms. Klein is a member of the Virginia and District of Columbia bars and the American Health Lawyers Association.

DANIEL F. MCINNIS, Partner
dmcinnis@akingump.com

Washington, D.C. **T** +1 202.887.4359 **F** +1 202.887.4288

Practice Areas:
Antitrust and Unfair Competition
Commercial Litigation
Class Action
Privacy and Data Protection
Food and Drug Law
Policy and Regulation

Bar Admissions
District of Columbia
Virginia

Clerkships
U.S.C.A., DC Circuit
U.S.C.A., 5th Circuit

Education
J.D. Georgetown University Law Center, cum laude, 1994
B.A. Yale University, 1989

Daniel F. McInnis' practice focuses on antitrust cases and government investigations, consumer protection matters and litigation, and civil lawsuits involving complex issues of federal practice and procedure.

Mr. McInnis principally concentrates on antitrust matters. He has broad experience in antitrust litigation, investigations and counseling. He has represented clients in civil and criminal antitrust litigation in both federal and state courts. He has counseled and represented clients on matters relating to mergers and acquisitions and related investigations by the Department of Justice and the Federal Trade Commission in diverse industries such as supermarket retailing, soft drinks, commodities, oil and gas, and advertising. In addition, he has had significant involvement in antitrust counseling and designing and implementing effective antitrust compliance programs. Mr. McInnis has represented clients in legislative matters involving antitrust law and policy.

Mr. McInnis also focuses on consumer protection investigations and enforcement actions by the Federal Trade Commission's Bureau of Consumer Protection and by state and local law enforcement officials, including the investigation of companies for deceptive or unfair acts or practices. He has also represented clients in private litigation under state consumer protection statutes and the Lanham Act. Mr. McInnis counsels clients on appropriate advertising and marketing practices.

Mr. McInnis has represented clients, both as plaintiffs and defendants, in a variety of complex civil litigation matters and class actions. His cases have included a variety of federal and state lawsuits involving complex, commercial controversies, at both the trial and appellate levels.

From 1994 to 1995 Mr. McInnis served as a law clerk for the Honorable Jerry E. Smith of the U.S. Court of Appeals for the 5th Circuit. From 1993 to 1994 he was an extern clerk for the Honorable James L. Buckley of the U.S. Court of Appeals for the D.C. Circuit.

Mr. McInnis received his B.A. in English in 1989 from Yale University and his J.D. cum laude in 1994 from the Georgetown University Law Center, where he was an editor of the *Georgetown Law Journal*. Prior to attending law school, he was a policy analyst for the Competitive Enterprise Institute, a Washington-based free market think tank. He is active in the ABA's Section of Antitrust Law, the Federalist Society and the Republican National Lawyers Association. Mr. McInnis is a member of the Virginia and District of Columbia bars.

JAMES R. TUCKER, JR., Partner
jtucker@akingump.com

Washington, D.C. **T** +1 202.887.4279 **F** +1 202.887.4288

Practice Areas: **Climate Change**
Policy and Regulation
Public Law and Policy
Privacy and Data Protection

Bar Admissions
District of Columbia
Georgia

Education
J.D. Mercer University Walter F. George School of Law, 1997
B.A. Washington & Lee University, 1992

Jamie Tucker has more than 15 years of political and policy experience. He combines this knowledge with a network of government contacts to provide strategic advice to and advocacy on behalf of clients at the federal and state levels.

Prior to joining Akin Gump in 1999, Mr. Tucker served as legislative counsel to Rep. Bob Inglis, R-S.C. In that capacity, he was responsible for advising the congressman on all issues before the House Judiciary Committee. He also served as an aide to former Speaker of the House Newt Gingrich in 1996 and to Sen. Paul D. Coverdell, R-GA, in 1993-94. Mr. Tucker also has significant political experience, having worked on the 2000 and 2004 Bush/Cheney campaigns, the 1996 Dole/Kemp campaign and the 1992 Bush/Quayle campaign. He also served in various capacities at the 2000 and 1992 Republican National Conventions. He has also worked for or volunteered on behalf of a number of Senate and congressional races and is active with the Republican Governors Association.

His practice in the public policy arena spans many disciplines including—

Strategic Advocacy

Mr. Tucker works collaboratively with clients to develop a comprehensive strategy to achieve their public policy objectives, whether they are offensive or defensive in nature. He combines an in-depth knowledge of the policy making process and an extensive network of contacts in Congress and the Administration to achieve results. He has worked effectively on behalf of such clients in the energy, healthcare, technology, telecommunications, transportation and agricultural sectors.

Congressional Investigations

The power of Congress to investigate is as broad as its power to legislate, and organizations engaged in such proceedings are confronted with a unique set of challenges. The legal proceedings involved in congressional investigations are distinct from those in any other forum, and investigations have political and public relations pitfalls as well. Mr. Tucker has helped clients navigate these proceedings while successfully protecting their legal, political and reputational standing.

Federal Marketing and Appropriations

Mr. Tucker works with clients to position themselves to secure federal appropriations and grants for meritorious projects. Competition for these funds is often intense and the process for securing them has grown increasingly complex. Mr. Tucker has a proven track record of working with clients to identify relevant sources of funding, developing compelling proposals to policy makers and navigating the process to ensure that key application and disclosure deadlines are met.

Additionally he works with clients to maximize opportunities for sales of products and services to federal and state governments. The public sector represents a significant opportunities for companies of all sizes and Mr. Tucker helps clients navigate the unique and often complex aspects of this market.

Mergers and Acquisitions (M&A) Political Counsel

Mr. Tucker works with companies and investors to identify and minimize the political risks associated with mergers and acquisitions. He has helped develop and execute targeted strategies to condition the environment in which a transaction is reviewed in including those deals subject to antitrust review by the Department of Justice (DOJ) or the Federal Trade Commission (FTC) or a national security review by the Committee on Foreign Investment in the United States (CFIUS).

Political Intelligence

Changes in the legislative and regulatory landscape in Washington can have a profound impact on a company's economic outlook. Mr. Tucker works with corporate managers and investors to identify and analyze the economic implications of policy decisions. He works to provide clients with real-time information and also to identify long-term trends that will impact a company's or sector's bottom line.

Grassroots / Stakeholder Advocacy

Mr. Tucker often manages grassroots or stakeholder advocacy campaigns on behalf of clients. Such efforts focus on identifying, educating and mobilizing local and state opinion leaders in support of a policy objective. This may involve providing community support for or opposition

to a regulatory filing or legislative proposal or simply advancing an organization's broader community relations objectives.

Local Counsel Management

Legislative or regulatory issues will often play out across multiple venues and jurisdictions simultaneously. Mr. Tucker works with clients to ensure that their positions are well positioned by identifying local counsel suited to the issue and coordinating messaging so that the client maintains a unified approach.

Mr. Tucker received his J.D. in 1997 from Mercer University, where he was presented the award for Outstanding Achievement in Legal Writing and his B.A. in politics in 1992 from Washington and Lee University. He is a member of the District of Columbia and Georgia bars.

APPENDIX:
SELECTED ARTICLES

The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 9 September 2011

Legislative Proposals Compete As Privacy, Data Security, And Breach Notification Continue To Draw The Attention Of Federal Policymakers

Francine E. Friedman, Jo-Ellyn Sakowitz Klein, James R. Tucker Jr. and Kristofer A. Ekdahl

AKIN GUMP STRAUSS HAUER & FELD LLP

Francine E. Friedman

Jo-Ellyn Sakowitz Klein

James R. Tucker Jr.

Kristofer A. Ekdahl

The Obama administration and Congress view regulations regarding privacy, data security and breach notification as areas where bipartisan agreement may be possible. Well over a dozen bills have been introduced this year alone, and federal agencies ranging from the Federal Trade Commission and the Department of Commerce to the Department of Homeland Security and the Department of Justice have added their input to the debate.

New proposals would change how data is collected, stored and used. They pertain to three areas that often overlap: online and point-of-sale privacy, mobile device and geolocation privacy, and data security and breach notification. The scope of recent proposals is sufficiently broad that a range of industries and sectors would be directly impacted. Retailers, website operators, banks, large employers, data brokers, online marketers, law enforcement, credit reporting agencies, nonprofit organizations and many other entities need to prepare for the possibility of new regulations.

Array Of Online And Point-Of-Sale Privacy Bills Introduced

Six bills pertain primarily to online and point-of-sale privacy. These bills impose new standards on the collection, use and sharing of consumer information. Key proposals include:

- Rep. Jackie Speier (D-CA): Do Not Track Me Online Act of 2011 (H.R. 654). This bill requires opt-out mechanisms for the collection or use of online and personal data.
- Sens. John Kerry (D-MA) and John McCain (R-AZ): Commercial Privacy Bill of Rights Act of 2011 (S. 799). This bill requires opt-out mechanisms for data sharing, as well as opt-in consent for the collection, storage or sharing of sensitive personal information.
- Rep. Bobby Rush (D-IL): BEST PRACTICES Act (H.R. 611). This bill is similar in structure to the Kerry-McCain proposal. It calls for opt-out mechanisms for data collection and storage, as well as opt-in consent for third-party information sharing.

Francine E. Friedman *is Senior Policy Counsel in Akin Gump's privacy and data protection practice and has a decade of government affairs and lobbying experience. She advises clients on a variety of issues including tax policy involving housing, energy and new markets tax credits; financial services reform; data security; and energy issues.* ***Jo-Ellyn Sakowitz Klein*** *is Senior Counsel and leads the firm's interdisciplinary privacy and data protection initiative. She devotes much of her practice to regulatory, transactional and legislative matters affecting the health industry. She also advises clients outside the healthcare sector that are affected by healthcare or privacy law and regulation.* ***James R. Tucker Jr.*** *is a Partner in the firm's data privacy and data protection practice and has 15 years of political and policy experience. He combines this knowledge with a network of government contacts to provide strategic advice to and advocacy on behalf of clients at the federal and state levels.* ***Kristofer A. Ekdahl*** *is a Senior Public Policy Specialist. All authors are resident in the firm's Washington, DC office.*

Please email the authors at ffriedman@akingump.com, jsklein@akingump.com, jtucker@akingump.com and kekdahl@akingump.com with questions about this article.

• Rep. Cliff Stearns (R-FL): Consumer Privacy Protection Act of 2011 (H.R. 1528). This bill allows consumers to opt out of having their personally identifiable information shared with third parties.

• Sen. John Rockefeller (D-WV): Do-Not-Track Online Act of 2011 (S. 913). As chair of the Commerce Committee, Sen. Rockefeller will play a central role in shaping Senate privacy proposals. His bill gives consumers the ability to opt out of having their online data tracked and stored. His proposal goes one step further than the aforementioned privacy bills by also imposing limits on data collection from mobile devices.

• Reps. Ed Markey (D-MA) and Joe Barton (R-TX): Do-Not-Track-Kids Act (H.R. 1895). Markey and Barton are co-chairs of the congressional Bi-Partisan Privacy Caucus. Their proposal forbids online companies from using personal information for targeted marketing to children, empowers parents to delete their children's digital footprint and requires parental consent for any data tracking online or on mobile devices.

Mobile Privacy And Geolocation Bills Becoming More Common

While the Rockefeller and Barton-Markey proposals touch on many aspects of consumer privacy, including mobile privacy, a second group of bills focuses solely on mobile devices. These bills restrict the collection and sharing of geolocation data. Key proposals include:

• Sen. Ron Wyden (D-OR) and Rep. Jason Chaffetz (R-UT): Geolocation and Privacy Surveillance (GPS) Act (S. 1212, H.R. 2168). Released as companion bills in the Senate and House, these bills prohibit companies from collecting or sharing geolocation information without the user's express consent.

• Sens. Al Franken (D-MN) and Richard Blumenthal (D-CT): Location Privacy Protection Act of 2011 (S. 1223). This bill requires any covered entity to offer up-front notice and receive informed consent from users to track their geolocation information.

• Sen. Patrick Leahy (D-VT): Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011). Sen. Leahy chairs the Judiciary Committee and has been active in privacy debates. Enacted in 1986, the ECPA restricts third-party access to private electronic communications, such as online activity and e-mails. Because the ECPA does not cover GPS-based information, Leahy's proposal adds geolocation information as a new class of private communications subject to the protections of the ECPA.

Data Security And Breach Notification Bills Gaining Traction

Seven bills have been introduced that primarily focus on data security and breach notification. These bills require entities that collect or store data to implement safeguards to protect data and create a standard for notifying government agencies and consumers if an organization's files are breached. Key proposals include:

• Rep. Mary Bono Mack (R-FL): SAFE Data Act (H.R. 2577). As chair of the Commerce, Manufacturing, and Trade Subcommittee, Bono Mack is one of the key leaders in the House. Her proposal requires businesses to notify consumers and the FTC after a breach is contained and assessed. It also calls for data minimization and stronger security, and it would entitle affected individuals to free credit monitoring services for two years.

• Sens. Rockefeller and Mark Pryor (D-AR): Data Security and Breach Notification Act of 2011 (S. 1207). This bill requires businesses and nonprofit organizations that store personal information to implement reasonable security measures and alert consumers when their data has been compromised. In the event of a breach, affected individuals would be entitled to free credit monitoring services for two years.

• Sen. Leahy: Personal Data Privacy and Security Act (S. 1151). This bill is similar to bills he has introduced in previous Congresses. His proposal calls for businesses to enact security procedures to protect sensitive data, and it creates a federal standard for notifying appropriate parties in the event of a breach.

• Sens. Tom Carper (D-DE) and Roy Blunt (R-MO): Data Security Act of 2011 (S. 1434). This bill requires entities that possess sensitive information to build safeguards, as well as to enact policies for investigating security breaches and notifying consumers when a substantial risk of identity theft or account fraud exists.

• Sen. Dianne Feinstein (D-CA): Data Breach Notification Act of 2011 (S. 1408). Unlike some other proposals in this category, this bill only applies to breach notification standards. This is the fifth consecutive session of Congress in which Sen. Feinstein has introduced a breach notification bill.

• Rep. Rush: Data Accountability and Trust Act (H.R. 1707). This bill mandates stricter data security policies and creates a national standard for breach notification.

• Rep. Stearns: DATA Act of 2011 (H.R. 1841). Stearns' security and breach notification bill is similar to Rush's in its call for tighter protections of data storage and a standard for notifying affected individuals and government authorities in the event of a breach.

Despite Obstacles, New Regulations May Still Be Implemented

A highly partisan atmosphere certainly clouds the prospects for congressional approval of new data security and privacy regulations. Moreover, the sheer number of bills complicates attempts to build a coalition behind a single proposal, and congressional committees continue to jockey for their claim to jurisdiction over these issues. Yet, given the loud drumbeat from privacy advocates and the seemingly incessant revelations of high-profile breaches, policymakers will continue to push forward in the areas of privacy, data security and breach notification regulations. Even in the absence of meaningful congressional action, the Obama administration may opt to enact its own changes based on its existing regulatory authority. The realm of consumer privacy and data security in the digital era is fast-evolving, and as federal policymakers try to keep pace, much is at stake for everyone involved.

Portions of this article originally appeared in BNA Daily Report for Executives, 139 DER B-1, 7/20/11, copyright 2011, and are reproduced with permission of The Bureau of National Affairs, Inc. (800-372-1033), http://www.bna.com.

BNA

Daily Report for Executives

Privacy

Data security and consumer privacy issues are gaining traction in Washington and the interest may yield a new regulatory framework, write Francine Friedman, Jamie Tucker, Jo-Ellyn Sakowitz Klein, and Kris Ekdahl of Akin Gump Strauss Hauer & Feld LLP. More than a dozen bills have been introduced this year, and the Federal Trade Commission and Department of Commerce have published their own recommendations. Covered entities should establish privacy and security policies, assess risks and assign oversight, and prepare workforces for future changes.

High-Profile Breaches Spur Congressional Activity on Privacy, Data Security Policy

BY FRANCINE FRIEDMAN, JAMIE TUCKER, JO-ELLYN SAKOWITZ KLEIN, AND KRIS EKDAHL

With a Republican-controlled House opposite a Democratic-controlled Senate, and presidential and congressional elections looming in less than sixteen months, few proposals of significance are capable of advancing to become law. Data security and consumer privacy, however, are hot-button issues that are gaining traction and may yield consensus for a new regulatory framework. Bipartisan and bicameral support exists in Congress for updated data security and privacy laws, and the Obama administration is actively engaged. New regulations could directly impact any entity that collects, stores, or shares data on a large scale. Data brokers, online marketers, advertising agencies, ad networks, retailers, banks and other financial services companies, media and publishing companies, automobile manufacturers, mobile application developers, companies selling consumer packaged goods, law enforcement, web browsers, large employers, website operators, credit reporting agencies, and nonprofit organizations (including universities) need to be aware of these policy debates and prepare for the possibility of new regulation in the near future.

A string of high-profile incidents has accelerated the drumbeat in Washington for increased regulation. Major corporations and even government entities have fallen victim to large-scale data breaches, and many mobile devices have been discovered to allow tracking and recording of users' locations (97 DER A-28, 5/19/11). Names, birth dates, Social Security numbers, e-mail addresses, passwords, locations, and even credit or debit card numbers increasingly seem at risk, fueling the anger of privacy watchdogs and galvanizing policymakers (85 DER A-3, 5/3/11).

 ISSN 0148-8155

Congress, Administration Respond to Breaches

Congress and federal agencies have scrambled to respond to privacy advocates' outcry for increased regulation. More than a dozen bills have been introduced this year, and the Federal Trade Commission (FTC) and Department of Commerce have published their own recommendations.

The proposals pertain to three areas that often overlap: online and point-of-sale privacy, mobile device privacy, and data security and breach notification. The scope of the various proposals is sufficiently broad that if enacted in part or in full, entities across the spectrum would be impacted.

With so much at stake, this is a critical moment for covered entities to educate themselves and consider adding their voices to the policy debate in Washington, D.C. Moreover, now is an ideal time for these groups to assess their privacy and security procedures to ensure compliance with legal and industry best practices frameworks currently in place on both the national and state levels.

This article will help covered entities navigate the evolving consumer privacy debate. An analysis is set forth of key pending regulatory proposals in Congress and the federal agencies, the practical implications of proposed regulations, how these proposals might interact with existing law, and what companies and nonprofit organizations should do today to comply with the complicated patchwork of privacy regulations currently in place.

Bills on Consumer Privacy, Data Security

Recent proposals pertain to three general topics.

First, consumer privacy bills seek to help consumers control what personal information is collected, used, stored, or shared based on their online and point-of-sale behavior. Second, mobile privacy bills seek to help consumers take control of what information is collected, used, stored, or shared based on their mobile device usage and their geolocation footprint. Third, data security and breach notification bills seek to implement new protocols for protecting data and to create a national standard for notifying affected individuals and government agencies when a breach has occurred. Some of the proposals under discussion by policymakers span more than one of these categories.

Various Approaches to Privacy Issues

Six bills have been introduced this year that pertain primarily to online and point-of-sale privacy. By browsing the internet or making purchases at a store, consumers reveal valuable information that is used to build user profiles based on their location, their tastes and interests, their contact information, and perhaps even their debit or credit card numbers. This data can be very valuable for behavioral marketers, which is why the practice of collecting and selling consumer data has grown so rapidly.

Privacy bills seek to change how consumer information is collected, stored, used, and shared, and what consumers are told about these practices. Bills regarding data *collection* call for opt-out or opt-in mechanisms that require express consent from the consumer before any personal information can be collected. Bills addressing data *storage* place new limits on the scope and duration of data retention and also impose new security procedures to safeguard information. Bills regarding data *use* and data *sharing* impose limits on the purposes for which data may be used, restrict with whom a data collector (e.g., a retailer) can share information, and set new standards for whether consumer consent or notification is necessary before information can be used in certain ways or shared with a third party.

Each of the privacy-focused bills differs slightly, but the above themes generally characterize this group of proposals. Key privacy proposals include:

- Rep. Jackie Speier (D-Calif.): Do Not Track Me Online Act of 2011 (H.R. 654). This bill would require opt-out mechanisms for the collection or use of online and personal data (30 DER A-6, 2/14/11).
- Sens. John Kerry (D-Mass.) and John McCain (R-Ariz.): Commercial Privacy Bill of Rights Act of 2011 (S. 799). This bill would require opt-out mechanisms for data use or sharing, as well as opt-in consent for the collection, storage, or sharing of sensitive personal information (126 DER A-15, 6/30/11).
- Rep. Bobby Rush (D-Ill.): BEST PRACTICES Act (H.R. 611). This bill is similar in structure to the Kerry-McCain proposal. It calls for opt-out mechanisms for data collection and storage, as well as opt-in consent for certain third-party information sharing.
- Rep. Cliff Stearns (R-Fla.): Consumer Privacy Protection Act of 2011 (H.R. 1528). This bill would allow consumers to opt out of having their personally identifiable information shared with third parties (94 DER A-2, 5/16/11).
- Sen. John D. Rockefeller IV (D-W.Va.): Do-Not-Track Online Act of 2011 (S. 913). As Chairman of the Senate Commerce Committee, Senator Rockefeller will play a central role in shaping Senate proposals on privacy and data security (90 DER A-15, 5/10/11). His bill would give consumers the ability to opt out of having their online data tracked and stored. Rockefeller's proposal would go one step further than the aforementioned privacy bills by also imposing limits on data collection from mobile devices.
- Reps. Ed Markey (D-Mass.) and Joe Barton (R-Texas): Do-Not-Track-Kids Act (H.R. 1895). Markey and Barton are co-chairmen of the Bipartisan Congressional Privacy Caucus. Their proposal would forbid online companies from using personal information for targeted marketing to children, would empower parents to delete their children's digital footprint, and would require parental consent for any data tracking online or on mobile devices (94 DER A-12, 5/16/11).

Mobile Device Privacy Getting Attention

While the Rockefeller and Barton-Markey proposals touch on many aspects of consumer privacy, including mobile privacy, a separate group of bills focuses solely on mobile devices. When users access GPS-enabled applications on their cell phones, smartphones, and tablet devices, they leave a valuable virtual trail of bread crumbs that can be used to reveal their present or past locations.

  DER ISSN 0148-8155

Proposals in this area seek to restrict the collection and sharing of geolocation data. The key proposals include:

- Sen. Ron Wyden (D-Ore.) and Rep. Jason Chaffetz (R-Utah): Geolocation and Privacy Surveillance (GPS) Act (S. 1212, H.R. 2168). Released as companion bills in the Senate and House, these bills would prohibit companies from collecting or sharing geolocation information without the user's express consent (116 DER A-26, 6/16/11).
- Sens. Al Franken (D-Minn.) and Richard Blumenthal (D-Conn.): Location Privacy Protection Act of 2011 (S. 1223). This bill would require any covered entity to offer upfront notice and receive informed consent from users to track their geolocation information (116 DER A-16, 6/16/11).
- Sen. Patrick Leahy (D-Vt.): Electronic Communications Privacy Act (ECPA) Amendments Act of 2011 (S. 1011). Senator Leahy is the Chairman of the Judiciary Committee and has been active in many aspects of the privacy debate. Enacted in 1986, the ECPA restricts third-party access to private electronic communications, such as online activity and e-mails. Because the ECPA does not cover GPS-based information, Leahy proposed this update to add geolocation information as a new class of private communications subject to the protections of the ECPA (96 DER A-22, 5/18/11).

Data Security, Breach Notification

Five proposals that primarily focus on data security and breach notification have been introduced in the 112th Congress. The aim of these bills is to require entities that collect or store data to take steps to prevent nefarious actors from accessing personal information and to create a standard for notifying government agencies and consumers if an organization's data is breached. Like some of the privacy bills discussed earlier, these proposals usually incorporate limits on the scope and duration of data storage, under the theory that if less data is stored, less data is at risk. However, security and notification bills impose additional regulations. First, they mandate security policies to prevent unauthorized third-party access to data. Second, they lay out procedures and time frames to alert affected individuals and government agencies when a data breach has occurred. Third, many of these bills require third-party data brokers to allow consumers to view their information and correct any errors.

The key bills in this area include:

- Sens. Rockefeller and Mark Pryor (D-Ark.): Data Security and Breach Notification Act of 2011 (S. 1207). This bill requires businesses and nonprofit organizations that store personal information to implement reasonable security measures and alert consumers when their data has been compromised; in the event of a breach, affected individuals would be entitled to free credit monitoring services for two years (116 DER A-23, 6/16/11).
- Leahy: Personal Data Privacy and Security Act (S. 1151). This bill is similar to bills Leahy has introduced in previous Congresses. His proposal calls for businesses to enact security procedures to protect sensitive data, and it would create a federal standard for notifying appropriate parties of a breach (111 DER A-7, 6/9/11).
- Bono Mack (R-Calif.): SAFE Data Act draft proposal. As chair of the Commerce, Manufacturing, and Trade Subcommittee, Bono Mack is one of the key leaders in the House. Her proposal requires businesses to notify consumers and the FTC within 48 hours of containing and assessing a breach. It also calls for data minimization, stronger security, and, like the Rockefeller-Pryor proposal, would entitle affected individuals to free credit monitoring services for two years (114 DER A-15, 6/14/11).
- Rush: Data Accountability and Trust Act (H.R. 1707). This bill mandates stricter data security policies and creates a national standard for breach notification (89 DER A-2, 5/9/11).
- Stearns: DATA Act of 2011 (H.R. 1841). Stearns' data security and breach bill is similar to Rep. Rush's in its call for tighter protections of data storage systems, in addition to setting a standard for notifying affected individuals and government authorities in the event of a breach (94 DER A-2, 5/16/11).

Administration May Push Forward

Given the plethora of bills and hearings on the topics of privacy and data security, Congress has clearly indicated its interest in passing new legislation this year. The sheer number of competing proposals and the potential for jurisdictional battles in Congress, however, complicates the path to overhauling privacy and data security laws. The legislative process is unpredictable and can be significantly influenced by external events, including data breaches and coverage of new and expanded uses of data. It is more likely that privacy advocates and industry can coalesce around a data breach notification proposal than agree on how to regulate the collection, use, and sharing of consumer information. It is noteworthy that business leaders recently testified before Bono Mack's subcommittee that they would support reasonable federal breach notification regulations.

The Obama administration is preparing its own blueprint for consumer privacy and data security in the event that Congress is unable to pass a meaningful bill. A White House cybersecurity proposal has been the subject of several hearings on Capitol Hill. While the administration's cybersecurity proposal primarily pertains to securing critical infrastructure against cyber attacks, it also calls for a national standard for breach notification.

Additionally, the FTC and the Department of Commerce have issued their own recommendations addressing online and point-of-sale privacy, mobile device privacy, data security, and breach notification. Core goals of the comprehensive FTC and Commerce plans include limits on what information can be collected and how long it can be stored, privacy policies that are shorter and simpler, persistent do-not-track preferences that follow a user from website to website, more transparency on the part of data collectors, and requiring companies to build security and privacy measures into products rather than layering on features as an afterthought. In the absence of meaningful congressional action on these points, it is possible that one or both agencies may utilize regulatory tools under their exist-

ing authority, such as rulemaking, enforcement actions, and issuing guidance. Action along these lines could be undertaken without an act of Congress.

Possible Impact of Increased Regulation

Congress and the administration are debating wide-ranging changes, and consequently the effects could touch nearly every consumer, business, and nonprofit organization in the country, either directly or indirectly. For instance, data privacy regulations, as currently envisioned in ''do not track'' and geolocation proposals, would significantly change operations for entities that purchase consumer information for behavioral marketing purposes. Third-party purchasers would be affected by stricter privacy regulations because they rely on the personal data that point-of-contact entities collect. New standards could change the advertising landscape online, on mobile phones, and on the ground because data privacy and geolocation bills could curtail data-driven, targeted marketing. Under many of the proposals, retailers, strategic advertising companies, and websites that host personalized ads would likely have a diminished ability to tailor and target their outreach to potential customers.

Practical Implications Could Be Far-Reaching

The true breadth of the new proposals is revealed by looking at the wide range of covered entities that could be affected.

The list includes browsers, ad networks, retailers, content websites, consumer research groups and data brokers, mobile network providers, mobile application developers, financial institutions, universities, nonprofit organizations, employers, and any other entity that collects and stores large amounts of personal information. If proposed online or point-of-sale privacy and geolocation regulations are adopted, this diverse group of covered entities would be limited in its ability to collect, store, use, or share consumer information. If data security and breach notification proposals are adopted, covered entities would be compelled to adhere to specific methods for storing consumer information and responding to breaches.

Practically speaking, new privacy regulations would create significant hurdles to sharing information, which would cause a substantial reduction in the information trade. With stricter privacy or geolocation restrictions, data collectors (e.g., a newspaper website or a mobile ''app'' provider):

- would collect less useful information about consumer preferences and interests;
- would be permitted to retain that information for a shorter duration than ever before; and
- may no longer be able to share the more relevant information with outside entities.

As a result, third parties will be less inclined to pay such a high premium for less robust consumer data files.

For example, advertisers strive to place their promotions in front of only those people who fit their profile of a likely customer. It can be more profitable to target 10 likely buyers than to broadcast to a random cross-section of 1,000 people. The information profiles that data collectors build and sell are what enable such targeted, high-yield, efficient marketing. If consumer profiles are no longer robust and insightful, they are no longer valuable.

The end result may lead to less data collector revenue from data sales, an impersonal user experience for consumers, lower yields on each advertising dollar spent, and ultimately a shift in the behavioral advertising business model. Web services that were sustained by advertising revenue may either go out of business or begin charging users for previously-gratis services. Free mobile ''apps'' that collected valuable GPS information may no longer be available. And Internet users will still see the same quantity of advertisements (if not more), but those ads will be less relevant to users' interests or needs.

Moreover, new breach notification regulations could have implications for consumer confidence, the reputations of breached entities, and internal investigations. If new rules lower the threshold at which a breach must be reported (in terms of the size or sensitivity of the data compromised), more breaches should be disclosed. Consumers who receive too many breach notifications that do not affect them may be lulled into complacency and not take proper action when a true risk is identified.

Possible Impact on Industry, Consumers

An increase in breach reporting can also undermine consumer confidence in institutions that store sensitive information, as a group. Whether or not a particular organization suffered a breach, the mere fact that a similar organization suffered one breach can have a corrosive effect on the universe as a whole. And for the entities that actually fall victim to a breach, the impact of negative publicity can be devastating. In either scenario, it is plausible that growing numbers of people would avoid sharing personal information with any outside entity. In the case of nonprofit organizations, that would mean fewer people contributing. In the case of businesses, that would mean fewer customers.

Regarding internal investigations after a breach, a quick notification deadline would give the breached entity very little time to conduct an internal review before the firestorm of journalists, government investigators, and angry customers make such a review infinitely more complicated. As a result, the organization may not be able to spot its vulnerabilities as quickly, leaving it susceptible to repeated attacks.

If implemented, these proposals would also translate into increased compliance costs and technical hurdles for both businesses and nonprofit organizations. Implementing new security features can be expensive and may necessitate an overhaul of computer systems, including migrating massive amounts of data from one platform to another. Not only that, but detailed security requirements may perversely increase the threat of breaches by providing would-be hackers with a road map of network security features. Potential complications arise with the privacy and geolocation proposals, as well. Deleting consumer data logs poses technical challenges if that data is stored on a ''cloud'' or on multiple networks. Adding opt-out or opt-in consents into every application would be cumbersome for data collectors, and such requirements would certainly reduce the number of consumers sharing their information.

  DER ISSN 0148-8155

Reasonable Uniform Breach Notification

For all of the implications that may be received negatively by data collectors and third party purchasers, one aspect of data security reform might be embraced by covered entities. Assuming strong state law preemption, a new federal standard would replace a disparate patchwork of state laws governing data security and breach notification. Generally speaking, reasonable uniform compliance requirements would be a welcome development for many organizations operating across state borders. In the realm of data security, a uniform federal standard may be palatable because complying with multiple state laws is untenable. Moreover, many organizations already have a strong self-interest in bolstering their internal security measures; therefore, a single federal security guideline could be welcomed by industry.

Considering Interplay With Existing Laws

One final item that covered entities need to monitor in the ongoing privacy debate is how new regulations might interplay with existing data security and privacy laws. The Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA) are some of the key federal privacy laws currently under enforcement.

Not all of the recent proposals mention existing federal statutes, but those that do (e.g., Leahy's data breach bill, Bono Mack's breach draft, and Stearns' privacy bill) indicate that existing statutes will trump the new proposals wherever overlap occurs. That may indicate Congress is likely to leave existing federal regimes like HIPAA and GLBA in place even if broader privacy and security regulations are adopted this year. Even so, entities that are currently covered by industry-specific regulations might still feel an additional regulatory burden if they collect, store, use, or share data for any purposes outside the purview of existing laws.

State privacy laws of similar scope would be preempted by most of the congressional proposals. Forty-seven states have their own breach notification laws, and every state has privacy or data security laws of some sort, which often differ from one state to the next. That patchwork of local laws places a high compliance burden on entities operating across state lines, so federal preemption may be a welcome change for some covered entities.

Speier's privacy bill is an exception, as it would *not* preempt state law if state law offers greater privacy protection than the federal law. The vast majority of congressional proposals, however, would supersede state laws wherever overlap occurs. If Congress passes a comprehensive privacy and data security bill this year, it is likely to reflect that consensus.

In the Meantime, Companies Should Act

In spite of all that is at stake in the ongoing policy debate regarding privacy and data security, the immediate priority for any covered entity should be to evaluate their policies vis-à-vis existing law and industry best practices. If an organization does not meet the standards already in place, adjusting to meet new regulations will be that much more difficult.

Unfortunately, evaluating a company's current position is made more complicated by the fact that no comprehensive federal privacy law governs the collection, use, storage, and sharing of consumer information. Rather, an ever-changing patchwork of sector-specific and data-specific state and federal privacy laws makes such compliance assessments difficult.

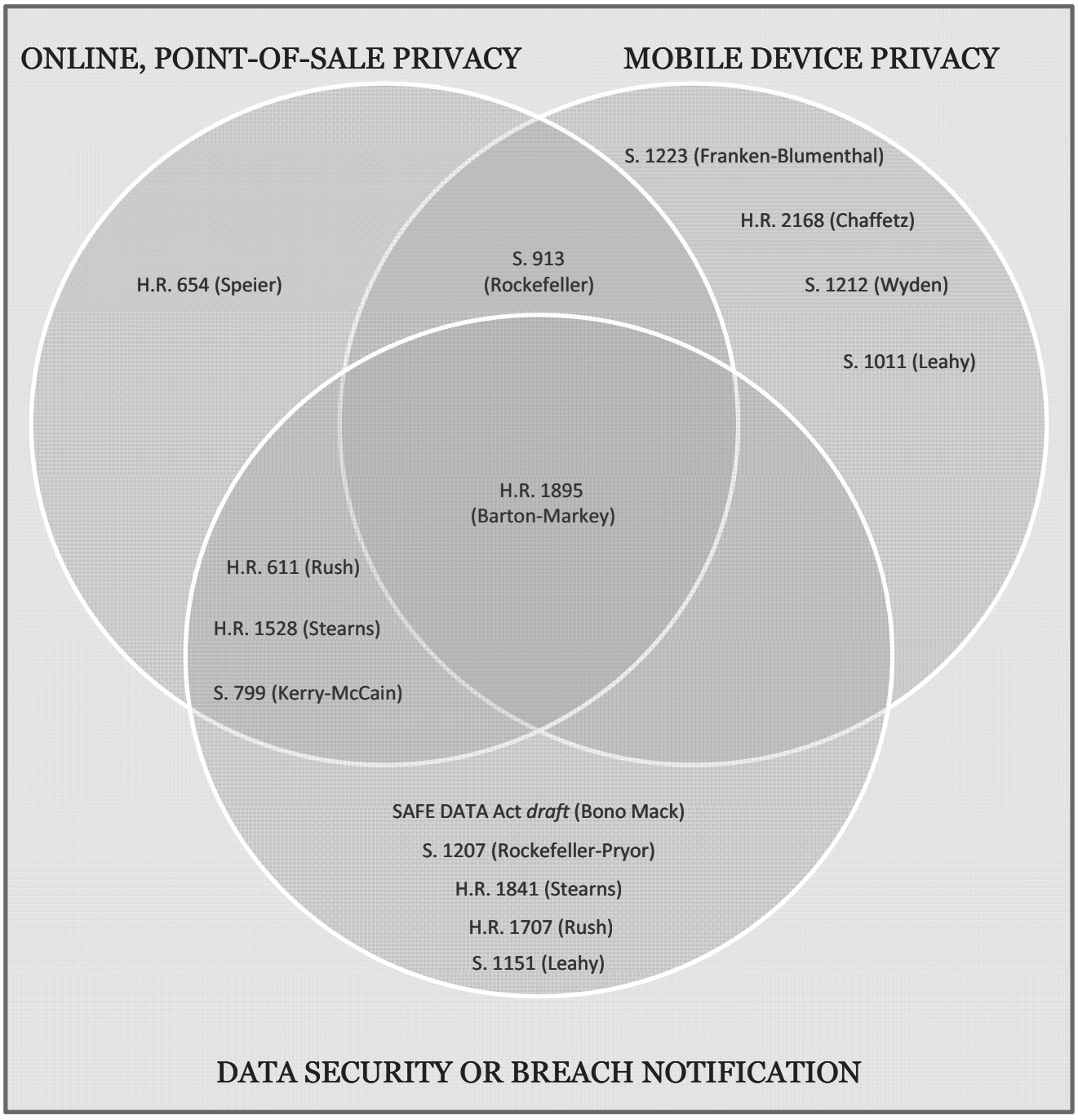
In light of these realities, some organizations may find it helpful to approach the issue from the perspective of attempting to identify steps that can be taken to minimize data privacy and security risks, rather than trying to develop a comprehensive checklist of all possible laws that may apply. While due attention must be paid to specific compliance mandates, privacy issues tend to be less linear, generally warranting a more dynamic approach.

Taking Steps to Minimize Exposure

Covered entities can take several steps to minimize exposure:

- First, companies should not underestimate the value of having reasonable written privacy and security policies. Policies and procedures should be reevaluated at regular intervals, as well as when incidents occur.
- Second, entities should conduct assessments to identify risks specific to their organizations and should be sure to incorporate low-tech and high-tech solutions.
- Third, entities should consider assigning one person responsibility over privacy and security concerns. The position of Chief Privacy Officer is becoming more common in the senior ranks of organizations.
- Finally, companies should train their workforces on privacy matters and ensure that all employees understand the importance of data security and privacy. Many breaches are the result of employee error, rather than external cyber attack.

The prospect for new federal data security and privacy regulations remains in flux. Given the attention that Congress and the administration have already dedicated to these issues, paired with the seeming inevitability of continued high-profile data breaches, it is plausible that a revamped national privacy framework could be agreed upon in the relatively near future. Yet with more than a dozen proposals already released from competing congressional committees, it remains difficult to predict what the final regulations might look like. Looking ahead, it is also important for companies to monitor or become engaged in the policy debate in Washington, D.C., and to better understand how proposals can impact their business. The realm of consumer privacy and data security in the digital era is fast-evolving, and as federal policymakers try to keep pace, much is at stake for all entities—and individuals—involved.



DER ISSN 0148-8155

The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 4 April 2011

Making Sense Of Recent HIPAA Enforcement Activity

Jo-Ellyn Sakowitz Klein and Kristen L. Henderson

AKIN GUMP STRAUSS HAUER & FELD LLP

In the first few months of 2011, the U.S. Department of Health and Human Services Office for Civil Rights issued its first-ever civil monetary penalty, against Cignet Health, for alleged privacy violations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), exacted a $1 million resolution amount from Massachusetts General Hospital for alleged HIPAA privacy violations, issued a budget request seeking substantial funding for HIPAA compliance and enforcement activities, and announced a new program to train state attorneys general to enforce HIPAA.

Many HIPAA-covered health care providers, health plans and health care clearinghouses are struggling to put these developments into perspective. The sheer size of the Cignet penalty – over $4.3 million – and the fact that the Office for Civil Rights (OCR) exercised its authority to assess civil monetary penalties (CMPs) for the first time led stakeholders to wonder if this development marked a sea change in enforcement attitudes. But concerns were tempered somewhat by the facts of the case, as the provider's abject noncompliance and refusal to cooperate with authorities made it seem like an outlier. The Massachusetts General Hospital (MGH) million-dollar resolution set the HIPAA community more on edge, as the breach – an employee accidentally left files containing medical records on a subway train while commuting – seemed like the type of incident that could occur despite an entity's sincere compliance efforts.

The OCR budget request and announcement of the new state attorney general training program added to an already tense environment. OCR is requesting about $46.7 million for fiscal year 2012, compared to its $44.3 million request for fiscal year 2011 and the $41.1 million enacted amount for fiscal year 2010. OCR is also reaching out to state attorneys general, offering substantial support in their efforts to enforce HIPAA using new authority granted under the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. OCR announced a series of intense two-day state attorney general training workshops, starting in April 2011, that will include instruction on issues ranging from HIPAA, HITECH and state legal requirements to investigative techniques for identifying and prosecuting potential violations to resources available to state attorneys general pursuing alleged HIPAA violations. Notably, HITECH allows courts to award damages (capped at $25,000 per calendar year for violations of the same requirement), as well as costs and attorney's fees, in such actions.

This article considers recent enforcement activity against the backdrop of the broader HIPAA enforcement timeline. When placed in context in this manner, the Cignet and MGH settlements seem to be more a continuation of a trend that has been slowly building over time than a shocking new development calling for drastic measures. Given the current environment, prudent covered entities should reinvigorate their HIPAA compliance efforts. This article continues to extract several lessons for covered entities from the enforcement timeline.

Putting Recent HIPAA Enforcement Actions Into Perspective

In the early days of HIPAA, outreach and education were the buzzwords of choice, as covered entities became acquainted with the new requirements. The promulgation of the interim final HIPAA privacy rule in December of 2000 marked the beginning of a period that would extend until compliance with the HIPAA security rule was mandated in 2005, during which covered entities focused on learning the regime and building compliance programs. Revisions to the regulations and the issuance of guidance documents made headlines. There were no seven-figure settlements, no resolution agreements with corrective action plans (CAPs) and no CMPs.

Providence: A Beginning

Then, in July 2008, the U.S. Department of Health and Human Services (HHS) announced the first HIPAA resolution agreement, in which Providence Health System and a pair of related entities (Providence) agreed to a detailed CAP and a $100,000 resolution amount for alleged privacy and security violations. The incident giving rise to the resolution agreement involved the loss of backup tapes, optical disks and laptops laden with unencrypted protected health information (PHI) on 386,000 individuals, which were removed from the entity's premises and left unattended in a car. Affected individuals were notified as required under state laws, and HHS received over 30 complaints. The CAP required Providence to revise its HIPAA policies and procedures, train workforce members accordingly, conduct monitoring and submit compliance reports to HHS for three years. This litany will become rather common. In its press release announcing the resolution agreement, HHS emphasized that Providence's cooperation with regulators allowed HHS to resolve the case without imposing a CMP. These words will take on an almost eerie significance, post-Cignet.

Rite Aid and CVS: Underscoring the Significance of Major Regulatory and Legislative Developments

Fast forward to February 2009, and the passage of the HITECH Act brings major changes to the HIPAA regime. Beyond enhancements to privacy requirements and the extension of HIPAA to business associates, HITECH dramatically increased penal-

***Jo-Ellyn Sakowitz Klein** is Senior Counsel in the health industry practice group and leads the privacy and data protection group at Akin Gump. **Kristen Henderson** is an Associate in the health industry practice group at Akin Gump.*

Please email the author at jsklein@akingump.com with questions about this article.

ties (raising maximums from $25,000 to $1.5 million), created an elaborate tiered penalty structure, added a new mandatory federal breach notification requirement and created new enforcement tools – including HIPAA enforcement authority for state attorneys general.

Almost in the same breath, on February 18, 2009, HHS announced that OCR had concluded a joint investigation with the Federal Trade Commission (FTC) into alleged HIPAA privacy violations by CVS pharmacies, and that the chain had agreed to pay a $2.25 million resolution amount and to take corrective action. The investigation began following media reports that CVS was disposing of pill bottles and other items containing PHI in open dumpsters. OCR's three-year CAP called for new policies and procedures relating to disposal of PHI (including workforce training and sanctions for noncompliance), internal monitoring and third-party audits. CVS entered into a separate consent decree with the FTC.

With the proposal of HITECH regulations in the summer of 2010 came another announcement – this time describing a settlement with Rite Aid that included a $1 million payment and similar CAP terms, plus an FTC consent decree, at the conclusion of a joint OCR/FTC investigation into similar allegations.

Management Services Organization: The Wheels Churn, Quietly

Then, somewhat quietly, in December of 2010, HHS announced a resolution agreement with a covered entity arising from facts revealed during a Federal False Claims Act investigation. Coordinating with the HHS Office for Inspector General and the U.S. Department of Justice, OCR entered into a resolution agreement and CAP with Management Services Organization (MSO), a covered entity that had allegedly shared PHI with a related entity for marketing purposes without the requisite authorization from affected individuals. HHS found that MSO intentionally did not have safeguards in place to protect information from such unauthorized use or disclosure. MSO agreed to pay $35,000 and implement a two-year CAP calling for policies and procedures, workforce training, monitoring and reporting.

Cignet: Outliers Beware

On February 22, 2011, HHS imposed its first-ever CMP for HIPAA violations: a penalty exceeding $4.3 million against Cignet. OCR found that Cignet failed to provide 41 patients with access to their medical records as required under HIPAA and, quite inexplicably, obstructed OCR's investigation. On receiving complaints from affected individuals, OCR initiated an investigation and notified Cignet in writing of its obligation to provide access to the requested records. Cignet failed to comply for months, even after OCR issued a subpoena. Only after OCR filed a petition to enforce its subpoena in a U.S. district court, and the court ordered Cignet to produce the records, did Cignet act. And in doing so, Cignet ran further afoul of HIPAA, producing records – without securing authorization – for several thousand patients above and beyond the 41 at issue. Before issuing its proposed determination, OCR gave Cignet the opportunity to submit evidence of any mitigating factors or affirmative defenses. Cignet failed to respond. In its final determination, OCR noted that Cignet made no efforts to resolve the complaints and, when calculating the amount of the CMP, considered the patients' inability to obtain continuing treatment and the fact that OCR was forced to issue a subpoena as aggravating factors. Applying the HITECH tiered penalty scheme, OCR assessed a $1.3 million penalty for the individual rights violations, plus a $3 million penalty for its "willful neglect" in failing to cooperate with the investigation.

Massachusetts General: The Wheels Churn, Not So Quietly

On the heels of the Cignet announcement, on February 24, 2011, OCR announced a $1 million settlement with MGH for alleged HIPAA privacy violations. An employee commuting on the subway inadvertently left behind files containing PHI for around 200 infectious disease practice patients, including records containing sensitive HIV/AIDS information. OCR's investigation indicated MGH failed to implement reasonable and appropriate safeguards where PHI is removed from the hospital's premises. MGH agreed to a CAP requiring the hospital to develop policies and procedures (notably, addressing USB and laptop encryption as well as physical removal and transport of PHI) and train workforce members accordingly. A specially designated monitor will oversee implementation of the CAP for a three-year period and report back to HHS.

There is no sign that the timeline will not continue from here. Indeed, the enforcement wheels continue to churn. OCR officials have noted that every complaint received by OCR is reviewed and analyzed, and an investigation is initiated if the facts and circumstances alleged indicate a compliance failure. As a result of the HITECH breach notification requirements, reports of sizeable breaches have been mounting, posted on a website for all to see. OCR has indicated that the agency is following up on those incidents. Presumably, some will be resolved through a long-term resolution agreement and CAP, while others will be addressed through voluntary compliance without sanctions. In the MGH press release, OCR Director Georgina Verdugo noted, "We hope the health care industry will take a close look at this [resolution] agreement and recognize that OCR is serious about HIPAA enforcement."

Some Lessons For Covered Entities

The enforcement trail yields a number of lessons for covered entities. First, do not underestimate the importance of having reasonable and appropriate written privacy and security policies and procedures. Policies and procedures should be reevaluated at regular intervals, as well as when incidents occur. Entities should conduct common sense assessments to identify risks specific to their organizations and should be sure to incorporate low-tech (as well as high-tech) solutions. Entities should learn from incidents endured by others and should review the OCR breach notification website, case examples and statistics – as well as the CAPs – for ideas regarding potential areas of weakness.

Covered entities should take care to comply fully with their own policies and procedures. The CAPs emphasize the importance of training – and retraining – workforce members. Especially in areas deemed HIPAA risks, policies and procedures should be tested through thoughtfully considered internal monitoring and audits. Sanction policies should be clearly documented and applied as circumstances dictate. All compliance efforts should be documented. This documentation will be critical should OCR initiate an investigation. And, of course, it is important to cooperate with OCR during any investigations.

The enforcement trail also suggests that fundamental individual rights, like the right to access, may be held particularly sacred; that OCR may be losing patience for sloppy safeguards that result in lost or stolen data (especially where PHI is taken off-premises); and that the agency may come down especially hard where sensitive information (like HIV/AIDS information) is involved. The Rite Aid and CVS settlements also convey the message that OCR expects data to remain secure throughout its lifecycle, from creation through destruction. And, as both Cignet and MGH learned most recently, it is not necessary to have thousands of individuals affected by an incident for an entity to face significant consequences under HIPAA and HITECH.

In conclusion, enforcement efforts have been building and do not seem likely to subside. Only with hindsight will we know for certain whether the recent confluence of events should be taken as a sign that OCR is shifting to a far more aggressive tact on HIPAA enforcement. Covered entities should learn what they can from the enforcement trail and reinvigorate HIPAA compliance efforts.

AKIN GUMP
STRAUSS HAUER & FELD LLP

Privacy and Data Protection Alert

FTC and Commerce Privacy Reports Point to Obama Administration Promoting Privacy Legislation

February 3, 2011

The Obama administration continues to focus on privacy issues, and this year's agenda will include continued enforcement efforts by the Federal Trade Commission (FTC), regulatory efforts led by the FTC and the Department of Commerce and a push for legislation. This alert focuses on this last point and briefly summarizes the policy highpoints driving these efforts as detailed in extensive reports issued in late 2010 by the FTC and the Department of Commerce.

FTC and Department of Commerce Make Headlines

The administration, through two key agencies—the FTC and the Department of Commerce—is attempting to shape the legislative debate over privacy issues. In December 2010, each issued a comprehensive report on its views and approaches to key privacy issues.

The FTC report, issued by its staff, is the latest in a series of privacy reports—some equally comprehensive, others industry- or issue- (identity theft, technologies, laws) specific. The FTC report, titled "Protecting Consumer Privacy in an Era of Rapid Change," is a preliminary report—meaning that the FTC is continuing to seek comments and reactions to the report and will likely issue a follow-on report. The Commerce report is called "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Framework." Both reports at a basic level advocate a more comprehensive and more legislative approach to privacy issues.

The FTC report is organized around three key principles based on what it terms a "privacy framework." This framework is not really a set of concrete proposals—a key exception is a proposal for a "do-not-track" law—but, for the most part, a set of basic aspirational goals.

The first goal is termed "privacy by design"—essentially, the recommendation that companies make privacy part of their "everyday business practices."

The second, "simplified choice," is the FTC's recognition that the "notice-and-choice" approach may not really be effective if consumers, as seems often to be the case, do not pay attention to the content of privacy notices. The FTC, not surprisingly, wants more effective choice.

Finally, the FTC urges "greater transparency," which seems to be a shorter version of the Fair Information Practices Principles (FIPP), i.e., there should be notice, access, disclosure and affirmative consent for changes in data use.

However, the FTC staff is careful to suggest that these concepts may have to be modified or applied through a sliding scale conditioned by the type of data or level of acceptance of the business practices at issue. Within these broad concepts, there are discussions of more- controversial issues such as the use and regulation of depersonalized data, self-regulation versus government enforcement, exclusions for less-sensitive data, consistency with existing privacy laws and correction of consumer data being held by companies.

www.twitter.com/akin_gump

The Commerce report is very similar in certain ways to the FTC report. The Commerce report advocates a generalized privacy approach it terms a "Dynamic Privacy Framework." This approach is basically a generalized privacy "bill of rights" based on an FIPP approach.

The report stresses that the focus of a baseline set of privacy principles would include transparency, i.e., better and more effective notice with effective limitations on purpose and specification uses as set forth in notices. It also would stress auditing and accountability.

These principles likely would be backed up by industry codes of conduct that may be enforceable through FTC actions. However, companies that followed the industry codes would be protected from regulatory actions by safe harbors.

Why the Different Approaches?

Different agencies do different things in different ways, and there are some key differences between the two reports.

First, Commerce is an executive agency—that is, it is run by its political appointees and, by extension, the administration. As a result, it can speak with one voice. The FTC, on the other hand, is an independent agency operated through the consensus of its five commissioners, two of whom, by law, have to be Democrats, two Republicans and one independent.

As a result, the Commerce report is simply more consistent in its overall approach. The FTC report is not, and, in fact, the Republican commissioners both filed concurring statements indicating that the proposals in the FTC staff's report are "flawed" or insufficiently based in empirical evidence. Consequently, the on-the-one-hand/on-the-other-hand quality of the FTC staff's report is most likely a reaction to countervailing practical, philosophical or even political concerns.

Further, Commerce is known as a business-friendly agency. Not surprisingly, the Commerce report, both in substance and, to a certain extent, in form, provides some industry-friendly recommendations, e.g., a national breach notification law that preempts state laws.

The Commerce report also recommends the creation within its hierarchy of a Privacy Planning Office. While the Commerce report is careful to acknowledge the role of the FTC and other parts of the U.S. government in developing privacy policy, the administration is clearly pushing for a more hands-on role through an executive agency.

Next Steps

The reports will be drivers for continued focus. Even as congressional committees will likely hold hearings on one or both of these reports to drive the dialogue and solicit feedback from stakeholders in advance of moving any legislation, each agency will try to use its report as a means of affecting legislative activity and expanding its power and authority.

CONTACT INFORMATION

If you have any questions regarding this alert, please contact—

Daniel F. McInnis
dmcinnis@akingump.com
202.887.4359
Washington, D.C.

James R. Tucker, Jr.
jtucker@akingump.com
202.887.4279
Washington, D.C.

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
202.887.4220
Washington, D.C.