DrinkerBiddle

Cyber Landscape

April 9, 2018

Steve Serfass

215.988.3313

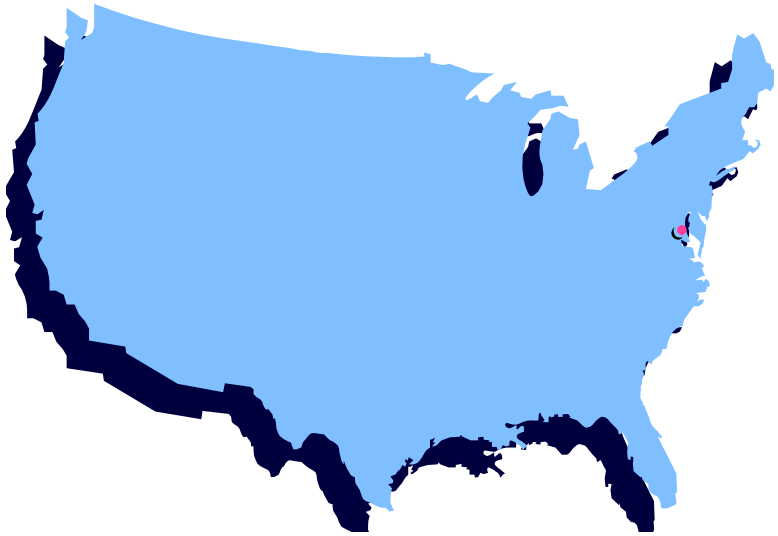
Stephen.Serfass@dbr.com

Headlines

- Regulatory advancement continues
- Enforcement is accelerating
- Breach litigation boundaries are being defined
- The next cyber risk is upon us

Legal Overview

Privacy and Data Security laws are a patchwork



Federal Law

State Law

Legal Overview

- Federal
  - No general federal cyber law
  - Sector specific laws (*e.g.*, GLB, HIPAA, COPPA)
  - Section 5 of FTC Act (unfair or deceptive acts or practices)
  - SEC – new cyber unit

Legal Overview

- State
  - Breach notification laws
  - Emergence of specific data security laws (*e.g.*, NY DFS Cybersecurity regulation, California financial privacy law)

Legal Overview: Federal Law

- Gramm Leach Bliley
  - Governs Nonpublic Personal Information (NPI) held by financial institutions
  - For insurers – personal, family, household purposes
- Other Federal laws that regulate personal information use/disclosure include: HIPAA; Electronic Communications Privacy Act; Stored Communications Act; Video Privacy Protection Act; Driver's Privacy Protection Act; Family Educational Rights and Privacy Act

Legal Overview: Federal Law

Section 5 of FTC Act (unfair or deceptive acts or practices)

F.T.C. v. Wyndam Worldwide Corp (3rd Cir. 2015)

- FTC alleged Wyndham engaged in unfair and deceptive trade practice in violation of the FTC Act by failing to maintain reasonable and appropriate data security for customers' sensitive personal information
- 3d Circuit agreed that FTC has authority under the "unfairness" prong of the FTC Act to bring enforcement actions against companies that the agency determines have unreasonable cybersecurity protections

Legal Overview: Federal Law

SEC has a New Cyber Unit

- September 2017, SEC announced creation
- Focuses Enforcement Division's cyber-related expertise on cyber-related misconduct
- December 2017, Unit filed first charges, for defrauding investors in the sale of crypto currency
- February 2018, SEC issued statement to assist public companies to meet cybersecurity disclosure requirements under federal securities laws

Legal Overview: Federal Law

NIST Framework

- National Institute of Standards and Technology (NIST) created a voluntary framework consisting of standards, guidelines, and best practices to manage cyber-security related risk
- February 2018, GAO issued review of the NIST framework
  - Analyzed sector-specific guidance and tools to facilitate implementation, and interviewed relevant federal and other officials
  - Found that most critical infrastructure sectors have taken action to facilitate adoption of the framework

Legal Overview: Federal Law

Regulatory Actions: OCR Steps up Enforcement

- Office for Civil Rights (OCR) enforces HIPAA
- Traditionally investigated breaches > 500 individuals; Recently broadened its approach
  - Factors to be considered:
    1. Size of the breach
    2. Theft or improper disposal of unencrypted PHI
    3. Breaches involving unwanted intrusions to IT systems (e.g., hacking), and the amount, nature and sensitivity of the PHI
    4. Instances where numerous breaches of a covered entity or business associate raise similar issues

DrinkerBiddle

Legal Overview: Federal Law

Regulatory Actions: OCR Enforcement

- April 2017 – CardioNet - 1,391 individuals - $2.5M
- February 2017 – Memorial Health Care System - 115,143 individuals - $5.5 M
- February 2017 – Children's Medical Center of Dallas – 6,262 individuals - $3.2M
- January 2017 – MAPFRE Life Insurance Co. of Puerto Rico – 2,209 individuals - $2.2M
- January 2017 – Presence Health – 836 individuals - $475K (1st HIPAA enforcement action for lack of timely breach notification)
- August 2016 – Advocate Health Care - 4 million records- $5.5M

Legal Overview: Federal Law

Regulatory Actions: CardioNet

- January 2012, employee's laptop stolen from parked car
- Contained ePHI of 1,391 individuals
- Following investigation of CardioNet's risk management processes, HHS determined CardioNet had no policies for the implementation of safeguards of ePHI

CARDIONET®
Get to the Heart of the Problem.

Legal Overview: Federal Law

Affinity Health Plan

- Non-profit issuer of managed care plans in the NY metropolitan area
- CBS affiliate purchased a copy machine previously leased by Affinity; found that it still stored PHI of 344K plan participants
- This breach led to an investigation into Affinity's compliance history and current practices

Affinity Health Plan
Dedicated to Excellence

Legal Overview: Federal Law

Affinity Health Plan

- HHS and Affinity agreed on a **$1.2 million fine** and a corrective action plan to ensure future compliance

Affinity Health Plan
Dedicated to Excellence

Legal Overview: State Law

Breach Notification Statutes

- 30 States –introduced or considered breach notification bills or resolutions in 2017
- 49 States – have enacted breach notification laws (Alabama is the only hold-out)
- DC, Guam, Puerto Rico and the Virgin Islands also have enacted breach notification laws

Legal Overview: State Law

Breach Notification Statutes

- Typically define: Data breach, protected information, notice requirements
  - Apply to ePHI generally, but some also apply to data in paper format
  - Some establish penalties and private rights of action
  - Recent revisions (1) expand definition of personal information (*e.g.*, biometrics); (2) require mitigation services (*e.g.*, credit monitoring); and/or (3) impose shorter deadlines for notification

Legal Overview: State Law

Breach Notification Statutes

- Some impose additional reporting requirements
- California requires insurers, insurance producers, and insurance support organizations to provide the Insurance Commissioner any notices submitted to the Attorney General's Office regarding security breaches

Legal Overview: State Law

- In addition to breach reporting statutes, states may have specific cybersecurity regulations
- The New York Department of Financial Services adopted 23 NYCRR 500 which imposes requitements on entities operating under DFS

Legal Overview: State Law

NYDFS Cybersecurity Regulation: Application

- Who is covered?
  - Direct v. Indirect Application
    - Direct: P&C, life, and health insurers, commercial banks, money transmitters, brokers
    - Indirect: "Third Party Service Providers" *with access to* Nonpublic Information

Legal Overview: State Law

NYDFS Cybersecurity Regulation: Application

- What information is covered?
  - PII, individual medical information, and sensitive company data
- General Requirements:
  - Cybersecurity Program: Policies and Procedures
  - Risk Assessment
  - Chief Information Security Officer (and other qualified personnel)
  - Third Party Service Providers – Compliance and Due Diligence

Legal Overview: State Law

NAIC Insurance Data Security Model Law

- **October 24, 2017** –NAIC adopted Insurance Data Security Model Law

  "[T]o establish standards for data security and ... investigation of and notification to the Commissioner of a Cybersecurity Event..."

  - Creates rules: data security, investigation, breach notification

  - Closely follows 23 NYCRR 500

A unified federal solution?

- February 14, 2018 - experts testified on the current data security/breach notification regulatory regime, before the House Financial Institutions and Consumer Credit Subcommittee
  - Urged Congress to adopt a data security standard to eliminate the patchwork of state laws
  - Testimony followed major data breaches involving Equifax and Uber

DrinkerBiddle

Living in a Post-Spokeo World:

Standing Issues in Breach Litigation

Breach Litigation: Difficulty Establishing Standing

- Standing to sue is one element of the cases and controversies requirement under Article III of the U.S. Constitution
- To establish standing, a plaintiff must allege:
  - **Injury-in-fact:** concrete, particularized, actual or imminent
  - **Causation**: fairly traceable to defendant's unlawful conduct
  - **Redressability:** likely to be redressed by requested relief

Breach Litigation: Difficulty Establishing Standing

- **General Rule:** No standing unless damages alleged
  - Examples of rejected arguments:
    - increased risk of identity theft
    - costs associated with credit monitoring
    - absence of misuse of information
    - reimbursed losses (*e.g.*, credit card charges)

Spokeo, Inc. v. Robins, 136 S.Ct. 1540 (May 16, 2016)

- Alleged Spokeo violated FCRA by publishing false information about Robins' financial condition, work experience, and family life
- Alleged those inaccuracies could negatively affect his job search by making him seem overqualified (*e.g.*, by exaggerating his personal responsibilities to a (non-existent) family)

Spokeo, Inc. v. Robins (cont.)

Issue: Whether Congress may confer Article III standing upon a plaintiff who has suffered no concrete harm by authorizing a private right of action based only on a procedural statutory violation

SCOTUS: Remanded to 9th Circuit

- Mere procedural violation of FCRA not enough to confer Article III standing
- Article III standing requires injury that is both particular *and* concrete

DrinkerBiddle

Breach Litigation: Example of Successful Pleading Pre-*Spokeo*

***John Lewert et al. v. P.F. Chang's China Bistro, Inc.*, (7th Cir. 2015)**

- P.F. Chang's system breached/credit card information stolen
- 7th Circuit - Relied on *Remijas v. Neiman Marcus*
  - Plaintiffs alleged injury-in-fact, satisfying the first element of standing, **because they pleaded increased risk of future fraudulent charges and identify theft based on the fact that their data had been stolen**

Breach Litigation: Difficulty Establishing Standing

***Khan v. Children's National Health System*, (D. Md. May 18, 2016)**

- Hackers had access to e-mail containing patients' personal information
- No indication patients' information was actually viewed, accessed, or copied, or was target of the phishing scheme
- Khan alleged violations of Consumer Protection Acts, and negligence, breach of implied contract, and unjust enrichment

Breach Litigation: Difficulty Establishing Standing

Khan v. Children's National Health System

- **Court:** In the data breach context, to allege an "injury-in-fact" arising from increase risk of identity theft, plaintiffs must show:
  1. Actual examples of use of fruits of data breach for identity theft, even if those examples involve other plaintiffs; or
  2. A clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud
- Therefore, Khan lacked standing, and the case was remanded to State court (not dismissed)

Breach Litigation: Difficulty Establishing Standing

Khan v. Children's National Health System

- Cited *Spokeo* in rejecting argument that violation of statutes and common law established standing

Court: "Article III standing requires a concrete injury even in the context of a statutory violation.... Although Congress may elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law... a bare procedural harm under a federal statute, divorced from any concrete harm, would not satisfy the injury-in-fact requirement"

Breach Litigation: Successful Pleading Post-*Spokeo*

***Galaria v. Nationwide Mut. Ins. Co.*, (6th Cir. 2016)**

- Hackers stole personal information of 1.1 million people; plaintiffs alleged they incurred costs to mitigate risk of identity theft

Court: "Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in the plaintiffs' complaints"

Breach Litigation: Successful Pleading Post-*Spokeo*

***Galaria v. Nationwide Mut. Ins. Co.*, (6th Cir. 2016) (cont.)**

Court: "Although it might not be 'literally certain' that plaintiffs' data will be misused, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable"

Takeaway: Heightened risk of identity theft and/or fraud due to data breach may constitute "concrete and particular injury"

Breach Litigation: Successful Pleading Post-*Spokeo*

***Attias v. Carefirst, Inc.* (D.C. Cir. 2017)**

Insured plaintiffs sued after insurer suffered a cyberattack in which their personal information was stolen;Plaintiffs attributed the breach to the insurer's carelessness

- Insurer moved to dismiss for lack of Article III standing
- **Court:** Plaintiffs' complaint sufficiently alleged sensitive information (including credit card and social security numbers) was stolen, which put Plaintiffs at substantial risk of identity theft

Breach Litigation: Successful Pleading Post-*Spokeo*

***Attias v. Carefirst, Inc.* (D.C. Cir. 2017)**

- The Court explained that in *Clapper*, the plaintiff's harm could only occur through a series of contingent events, none of which was alleged to have occurred at the time of the lawsuit; In the present case the unauthorized party already accessed personal identifying data and the harm is less speculative
- Insurer filed a Petition for Writ of Certioari to the U.S. Supreme Court, which was denied February 20, 2018

Breach Litigation: Unsuccessful Pleading Post-*Spokeo*

***Vigil v. Take-Two Interactive Software, Inc.* (2d Cir. Nov. 2017)**

Plaintiffs alleged violations of BIPA stemming from the collection of biometric data for use in a personal avatar for the NBA 2k15 and NBA 2k16 video games

- Players of the game consented to scanning and use of their face before the avatar could be created

Breach Litigation: Unsuccessful Pleading Post-*Spokeo*

Vigil v. Take-Two

Court: Plaintiffs failed to raise a material risk that their biometric data will be improperly accessed by third parties; Therefore, Plaintiffs did not establish a "risk of harm" sufficient to constitute injury-in-fact

- Cited *Spokeo* in reaching this decision
- Dismissal based on lack of Article III standing affirmed

Breach Litigation: Successful Pleading Post-*Spokeo*

***In re: Horizon Healthcare Servs. Inc. Data Breach Lit.* (3d Cir. Jan. 20, 2017)**

- A Horizon company-owned laptop containing 89,900 insureds' PII was stolen from an employee's car
- Plaintiffs alleged violations of FCRA because the incident "placed [them] at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud"

Breach Litigation: Successful Pleading Post-*Spokeo*

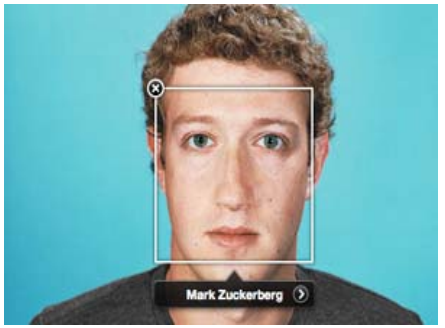
In re: Horizon Healthcare Servs.

- Horizon asserted Plaintiffs did not have standing based upon allegation of threat of future harm
- **Court:** Plaintiffs have standing because there is a concrete harm alleged, which FCRA expressly protects against
- "*Spokeo*... does not state that it is redefining the injury-in-fact requirement. Instead, it reemphasizes that Congress has the power to define injuries that were previously inadequate at law"

Breach Litigation: Successful Pleading Post-*Spokeo*

***Patel, et al. v. Facebook, Inc.*, (N.D. Cal. February 26, 2018)**

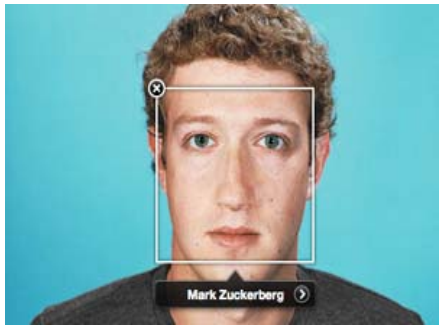
- **Plaintiffs**: Alleged Facebook's "Tag Suggestions" feature constitutes unauthorized collection and use of biometric data in violation of the Illinois BIPA
- BIPA drives the standing analysis; Court ultimately determined Plaintiffs have standing



Breach Litigation: Successful Pleading Post-*Spokeo*

***Patel, et al. v. Facebook, Inc.*, (N.D. Cal. February 26, 2018)**

- Cited *Spokeo* - alleged procedural statutory violation can by itself manifest concrete injury, where Congress conferred the procedural right to protect a plaintiff's concrete interests and where the procedural violation presents 'a real risk of harm' to that concrete interest
- State legislatures are equally well positioned to determine when an intangible harm is concrete injury



Breach Litigation: Successful Pleading Post-*Spokeo*

***Patel, et al. v. Facebook, Inc.*, (N.D. Cal. February 26, 2018)(cont.)**

- BIPA codified right to privacy in personal biometric information; Legislature determined violation of BIPA's procedures would cause actual and concrete harm
- Violation of BIPA constitutes a concrete injury and is enough for Plaintiffs to have standing under Article III

Breach Litigation Post-*Spokeo*

- Pleadings alleging an increased risk of identity theft and reasonable costs of credit monitoring **may** satisfy Article III standing after *Spokeo*
- What seems clear: pleadings that do not allege misuse of information, or intent of misuse will not establish standing
- *Spokeo* does not curtail Congress' ability to pass a statute that provides a private right of action for intangible harm; likewise state legislatures

The Next Wave of Cyber Risks/Exposure:

Biometrics

"Authentication techniques relying on measurable physiological and individual human characteristics that can be verified using computers"

By 2019, it is estimated that _____ biometric applications will be downloaded each year.

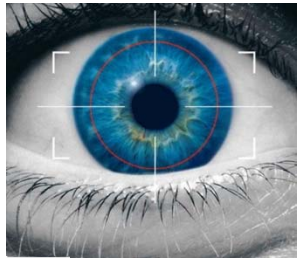
770 million

(compared to 6 million in 2015)

Two Types

- Behavioral
  - Signature, gait, lip motion, etc.

- Physiological
  - Fingerprints, iris, hand geometry, etc.



Variety of Uses

- Limit/provide physical access
- Apple TouchID (fingerprint), Samsung Iris Recognition Technology (fingerprint + iris)
- New York DMV Facial Recognition: Used to confirm identity and weed out individuals who should not get a license

Cyber risk: Biometric Breaches

Hacker Steals Fingerprint from Photo, Suggests Politicians Wear Gloves in Public

- Hacker used a high-resolution picture of politician's hand and "freely available commercial software" to recreate her fingerprint

Federal Regulation

- FTC: Released nonbinding privacy guidelines for use of facial recognition technology

  -"Privacy by design"

  -Data security controls & data destruction process

  -Consumer notice

  -Express consent for use outside of original purpose

State Regulation

Illinois Biometric Information Privacy Act

- Creates private right of action against businesses that fail to satisfy BIPA's requirements with respect to collection and use of biometric information
- Requirements:
  - Have a written policy
  - Obtain informed consent
  - Do not sell the data
  - Protect the data

BIPA LITIGATION: Statutory Standing

***Rosenbach v. Six Flags Entm't Corp.*(Ill. App. December 21, 2017)**

- Plaintiff alleged violation of BIPA, based on taking thumbprint without written consent in the purchase of season pass to Six Flags
- **Issue:** whether a party is "aggrieved" and may bring an action for liquidated damages or injunctive relief, when the only injury is violation of the notice and consent requirements of the statute

BIPA LITIGATION: Statutory Standing

Rosenbach v. Six Flags

- **Court:** Must allege some injury or adverse effect over the collection of biometric data to be "aggrieved"
- Thus, every technical violation of BIPA is not actionable; There must also be allegation of injury or adverse effect in addition to violation of the statute

BIPA Litigation

- **United Airlines and American Airlines** – Employees allege airlines use employee time clocks to collect biometric information (fingerprints and hand scans)

- **Hyatt** – Alleged violation of BIPA based on collecting and storing employees' fingerprints

BIPA Litigation

- **Bob Evans Restaurants -** Employees alleged violation based on requiring workers to provide their fingerprints, and then storing the prints
- **Shutterfly -** Allegedly collected facial recognition data without fulfilling BIPA requirements

Impact for Insurers

- Recognize coming biometric regulation:
  - States will look to BIPA & are likely to enact a similar law:

(1) Texas enacted Tex. Bus. & Comm. Code § 503.001 - which is very similar to BIPA

(2) Washington enacted a statute similar to BIPA codified in Title 19, Chapter 19.375 of the Revised Code of Washington.

Impact for Insurers

- Bills pending in additional states including Alaska, Connecticut, New Hampshire and others.
- **AK:** Regulates collection, retention, and use of biometric data
  - Requires "full consent"
  - Comprehensive biometric data definition
  - Allows for private right of action
- **CT:** Prohibits retailers from using facial recognition software for marketing
- **NH:** Establishes a committee to determine appropriate level of regulation for collection and use of biometric information.

Impact for Insurers

- Privacy Implications
  - Once stolen, it's gone forever
  - What is the appropriate remedy?
- Do current cyber liability policies address the risk?

DrinkerBiddle