July 18, 2018

Managing Legal Risk in the Information Era – Emerging Trends in Data Privacy and Cybersecurity Litigation and Enforcement

Colleen Brown, Partner, Sidley Austin LLP

Chris Fonzone, Partner, Sidley Austin LLP

Ilona Levine, CIPP/US, Sr. Corporate Counsel and DPO, Privacy, Cybersecurity and Compliance, OVH US

Danielle Carter, Associate General Counsel Ethics & Compliance, Smiths Group plc

SIDLEY

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

We are living in the midst of a social, economic, and technological revolution. How we communicate, socialize, spend leisure time, and conduct business has moved onto the Internet. The Internet has in turn moved into our phones, into devices spreading around our homes and cities, and into the factories that power the industrial economy. The resulting explosion of data and discovery is changing our world.

Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values,* May 1, 2014

Given these technological advances, nearly every day brings a new data privacy or cybersecurity story . . .

Data Breaches (Snowden, OPM, Target, Equifax, NSA, etc., etc., etc.)

Cross-Border Data Access and Sharing

Congressional Focus on Social Media

Artificial Intelligence and Machine Learning

The Internet of Things (and Bodies (and . . .))

Ubiquitous Encryption

Election Security

The Blockchain

Commercial Use of Customer Information

Cyber War

. . . and new legal issues.

Time works changes, brings into existence new conditions and purposes. Therefore, a principle, to be vital, must be capable of wider application than the mischief which gave it birth. . . . The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.

Olmstead v. United States, 277 U.S. 438, 472-74 (1928) (Brandeis, J., dissenting)

A Perfect Example: The Supreme Court's Recent Decision in *Carpenter v. United States* (Decided June 22, 2018)

- 5-4 decision resolves the question whether the government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.
- Decision was narrow, recognizing that a privacy interest continues to exist in cell phone records held by carriers. The decision is in tension with the third party doctrine from *Miller,* 425 U. S. 435 (1976) (no expectation of privacy in financial records held by a bank), and *Smith,* 442 U. S. 735 (1979) (no expectation of privacy in records of dialed telephone numbers conveyed to telephone company).
- Extensions of *Carpenter* could eventually further undermine the third party doctrine, although the Court does not do so here.
- The intellectual ground of U.S. privacy law remains uncertain:
  - Property is a concern because the Fourth Amendment (1792) protects "[t]he right of the people to be secure in *their* persons, houses, papers, and effects, against unreasonable searches and seizures."
  - A majority of the Justice accepts that expectations of privacy exist beyond property interests, but likely two would limit privacy to conceptions of property (albeit perhaps expanded notions of IP) and at least two would scrap the third-party doctrine entirely.
- Practically, this may help the EU's view of U.S. privacy law and could support stability on international transfers generally and the Privacy Shield review in particular.

Agenda

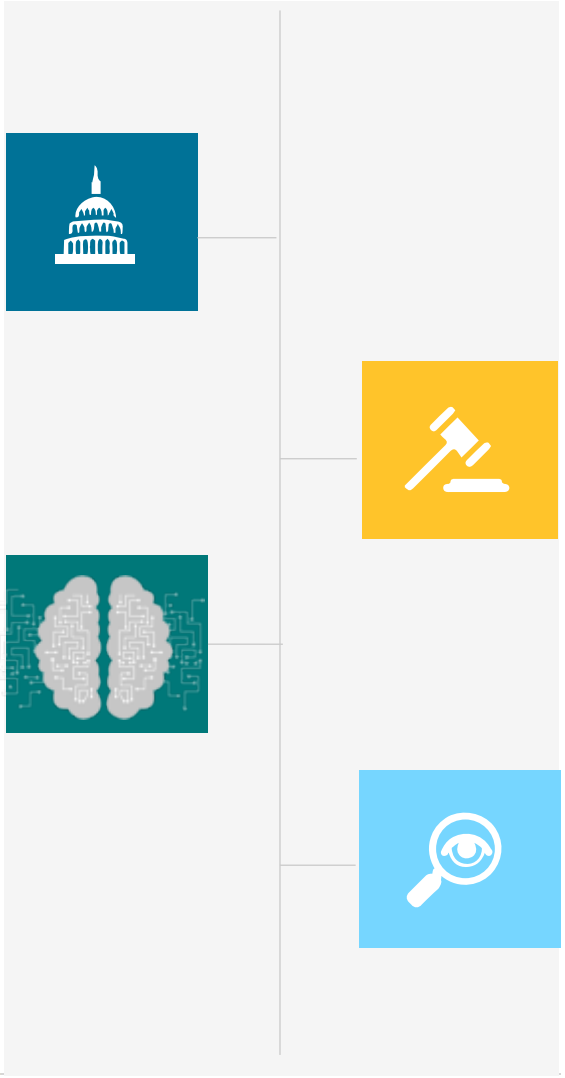
Key U.S. Regulatory Trends

- The SEC-led Focus on Cyber Governance
- The FTC Leads the Way in Terms of Federal Privacy and Information Security Regulation
- States Serve as "Laboratories of Democracy"

Other Key Trends

- Privacy and Cybersecurity Litigation
- B2B Trends
- Evolving International Standards, Including the GDPR

What the Future Holds



U.S. Regulatory Trends

Although there has been no comprehensive, national-level data privacy or cybersecurity legislation, the legal landscape is still dynamic.

- SEC guidance on cyber disclosures
- FTC and state unfair and deceptive practices
- Federal data security and data breach notification laws applicable to personal information (e.g., HIPAA/healthcare, GLBA/financial, ECPA/communications, CFAA/computer fraud)
- State data security and data breach notification laws
- State privacy laws (e.g., biometric privacy laws, social media privacy laws, right to be forgotten)
- Increasing International Obligations – GDPR, China
- Private litigation
- Numerous specific privacy and security statutes and agencies
- Company policies, industry standards, voluntary codes

Cyber Governance

Cyber Governance – SEC Focus on Public Disclosures

Boards (and Audit Committees) have a duty to provide oversight of SEC disclosures; SEC has focused on adequate public disclosure

2009
- SEC amended rules to require greater disclosure about the Board's role in risk oversight generally.

2011
- SEC issued guidance on disclosure obligations relating to cyber-security risks and incidents (including, depending on the circumstances, business description, risk factors, MD&A, legal proceedings and financial statements).

2014
- Commissioner Aguilar stated, "directors should be asking themselves what they can, and should, be doing to effectively oversee cyber-risk management."

2017
- Chairman Clayton says: "[i]ssuers should consider whether their publicly filed reports adequately disclose information about their risk management governance and cybersecurity risks, in light of developments in their operations and the nature of current and evolving cyber threats."

2018
- SEC releases guidance making clear that corporate insiders may not trade while in possession of nonpublic information regarding a significant cyber incident, and that companies should have policies in place to guard against such activity.

Cyber Governance – SEC Focus on Public Disclosures (II)

The February 2018 Guidance suggests that companies consider the following factors when evaluating cybersecurity risks for disclosure:

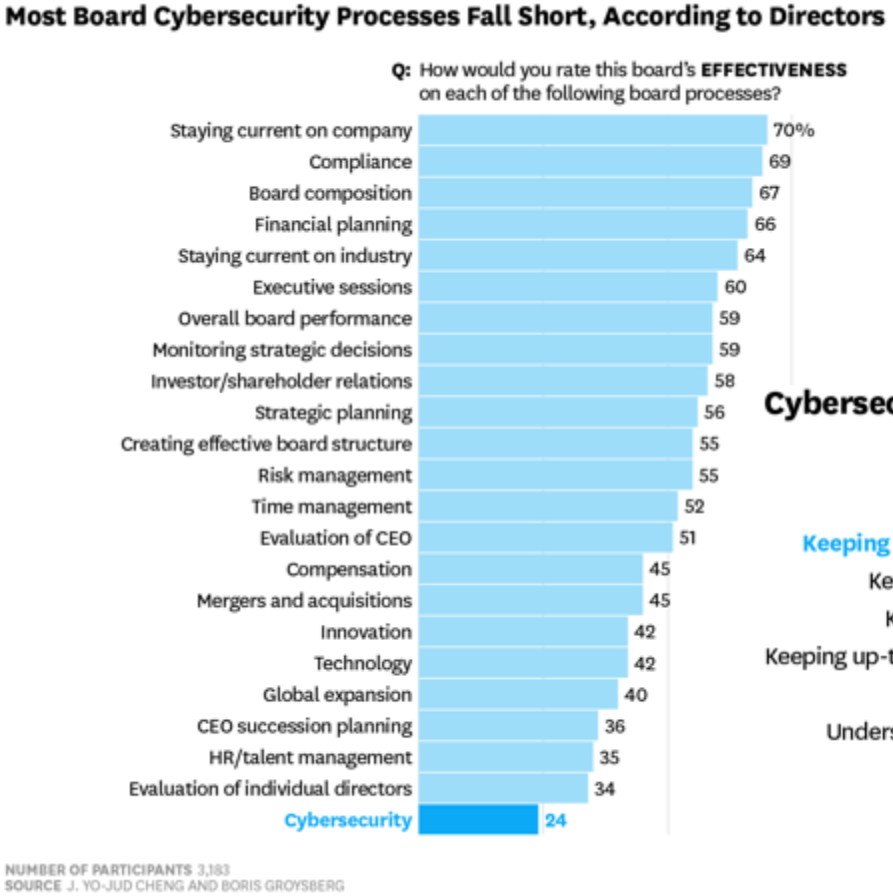
- Occurrence, frequency and severity of prior cybersecurity incidents;
- Probability and potential magnitude of cybersecurity incidents;
- Adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs;
- Aspects of the company's business and operations that give rise to material cybersecurity risks (including industry-specific risks and third-party supplier/service provider risks);
- Costs associated with maintaining cybersecurity protections (such as cyber insurance coverage or service provider payments);
- Potential for reputational harm;
- Existing or pending laws and regulations that may affect the cyber requirements and the associated costs to companies; and
- Litigation, regulatory investigation and remediation costs associated with cybersecurity incidents.

Cyber Governance – New York DFS Regulations

In 2017, DFS regulations are "first in the nation" regulation to impose prescriptive and specific cybersecurity requirements for financial sector (i.e., DFS-regulated entities). The requirements include:

- **Cybersecurity program and policies, plus risk assessment:** Must adopt cybersecurity program and policies, including a written incident response plan and risk assessment.
  - IRP must address several key points, including: (1) the **internal processes** for responding to an event; (2) the definition of **clear roles, responsibilities** and levels of **decision-making authority;** (3) external and internal **communications** and information sharing; and (4) **documentation and reporting** regarding Cybersecurity Events and related incident response activities.
  - As these content requirements make clear, incident response now, formally, must **explicitly contemplate multiple key stakeholders – not only** IT, Legal and Compliance, but also Communications, HR, Corporate Security, Government Relations and most importantly, lines of reporting up to Senior Management and Leadership.
- **Designation of CISO:** Implementing and overseeing the program and policies; annual report to the board/equivalent governing body.
- **Technical controls:** Encryption of data at rest and in transit (unless compensating controls), access controls, and multi-factor authentication.
- **Annual certification:** Annual written certification of compliance to DFS; must maintain all records and data supporting certification for five years in order to permit examination by DFS.

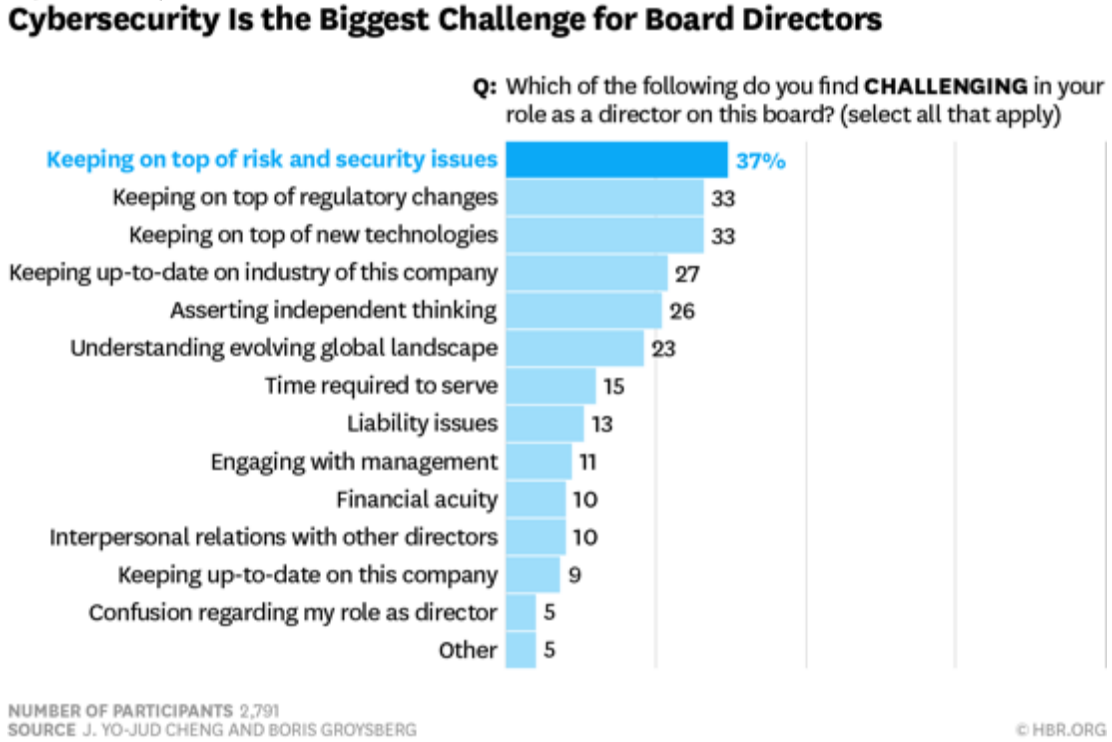
Cyber Governance – Boards Still See an Issue



Percentage that rated each process as "above average" or "excellent"

J. Yo-Jud Cheng & Boris Groysberg, Harvard Business Review (February 22, 2017)

"Why Boards Aren't Dealing with Cyberthreats"



Cyber governance – what are Boards doing?

Recognizing that cybersecurity is an enterprise-wide, and not just IT, issue

- All C-functions have some role to play, but needs to be clear ownership
- Key role for General Counsel

Ensuring that they can provide direction and oversight, not micromanagement

- Full board should receive briefing at least annually on enterprise-wide cyber risk and cybersecurity investment
- Many boards have started to draft policies or charters establishing Cybersecurity Committees

Adopting appropriate frameworks to make informed judgments about risk

- Key example: NIST *Framework for Improving Critical Infrastructure Cybersecurity*, which is now used by 1/3 of U.S. companies surveyed by NACD
- Framework describes basic cybersecurity functions and steps at various levels

Increasing director knowledge and expertise regarding cybersecurity

- Directors with technical knowledge
- Director education or Board-level table-top simulation on cybersecurity challenges

Ensuring that cyber risk is taken into account in M&A due diligence, reps and warranties

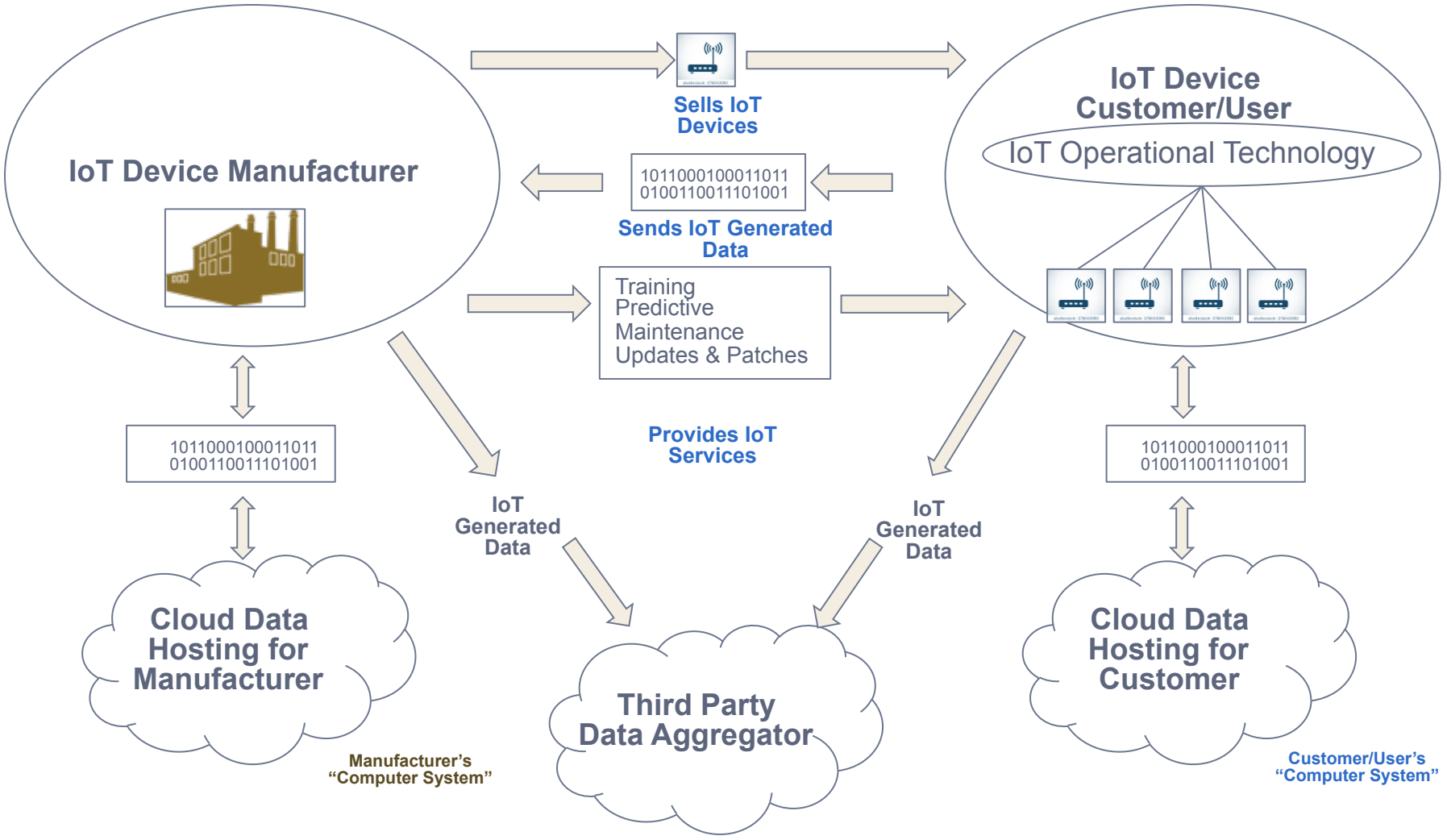
Federal Privacy and Information Security Regulation

FTC's Flexible Enforcement Power

- Section 5 of the FTC Act empowers it to protect consumers against "unfair or deceptive trade practices" – which the FTC applies to regulate privacy and data security (along with COPPA, FCRA)
  - *Wyndham* decision upheld FTC general authority to bring an unfairness or deception suit based on allegations of lax data security practices
  - Court acknowledged flexibility was particularly well suited to monitor fast moving technology and data practices
- FTC also enforces Fair Credit Reporting Act which has both direct relevance to certain applications of Big Data analytics, and may serve as guide for prospective approaches to Big Data
  - Notice of adverse decisions based on consumer reports
  - Limitations on data use and sharing
- Former FTC Commissioner (now at Microsoft) Julie Brill lead seminar series about threats of big data analytics, and supports a "take back your data" initiative..
- FTC pushed increased government focus generally on data brokers

The Law of Big Data Today

How does Notice and Choice work in this environment?



FTC's Informational Injury

Attempting "to identify, articulate, and categorize the types of harm that may result from automated decision-making" and "algorithmic discrimination."

A Taxonomy of New Harms

- Harms range from illegal to unfair
- Includes “societal” or “collective” harms with group impacts

Potential Mitigation Sets

Harms	Description	Mitigation Tools
Individual Harms – Illegal		
Employment Discrimination Insurance & Social Benefit Discrimination Housing Discrimination Education Discrimination Credit Discrimination Differential Pricing Individual Incarceration	Existing law defines impermissible outcomes, often specifically for protected classes	• **Data methods** to ensure proxies are not used for protected classes & data does not amplify historical bias • **Algorithmic design** to carefully consider whether to use protected status inputs & trigger manual reviews • **Laws & policies** that use data to identify discrimination
Individual Harms – Unfair (with illegal analog)		
Employment Discrimination Insurance & Social Benefit Discrimination Housing Discrimination Education Discrimination Credit Discrimination Differential Pricing Individual Incarceration	Individual harms that could be considered illegal if they involved protected classes, but do not in this case	• **Business processes** to index concerns; ethical frameworks & best practices to monitor & evaluate outcomes • **Laws & policies** include tools like DPIAs to measure impact or enable rights to explanation
Collective/Societal Harms (with illegal analog)		
Differential Access to Job Opportunities Differential Access to Insurance Benefits Differential Access to Housing Differential Access to Education Differential Access to Credit Differential Access to Goods & Services Disproportionate Incarceration	Group level impacts that are not legally prohibited, though related individual impacts could be illegal	• Same as above section • **Laws & policies** should consider offline analogies & whether it is appropriate for industry to identify & mitigate
Individual Harms – Unfair (without illegal analog)		
Narrowing of Choice Network Bubbles Dignitary Harms Constraints of Bias Constraints of Suspicion	Individual impacts for which we do not have legal rules. Mitigation may be difficult or undesirable absent a defined set of societal norms	• **Business processes** to index concerns, ethical frameworks & best practices to monitor & evaluate outcomes • **Laws & policies** should consider whether it is appropriate to expect industry to identify & enforce norms
Collective/Societal Harms (without illegal analog)		
Narrowing of Choice for Groups Filter Bubbles Stereotype Reinforcement Confirmation Bias Increased Surveillance of Groups	Group level impacts for which we do not have legal rules or societal agreement as to what constitutes a harm	• Same as above section

Key

Loss of Opportunity | Economic Loss | Social Stigmatization | Loss of Liberty

FUTURE OF PRIVACY FORUM

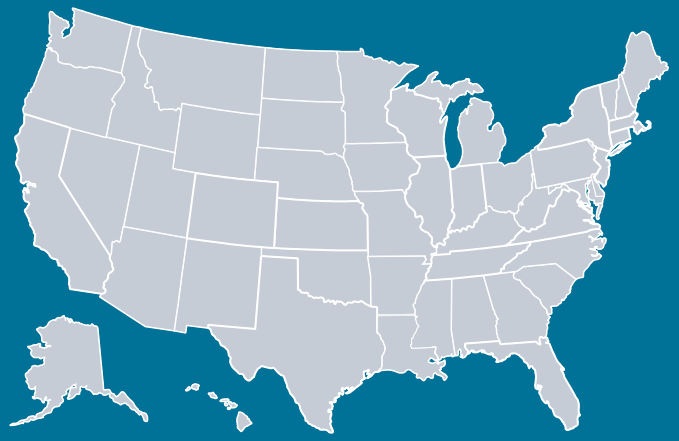
FTC Has Been Increasingly Active in Using Its Authority in Cases Involving Cutting-Edge Information Technologies

- It has brought data/technology-related enforcement actions for:
  - Providing insufficient notice to consumers (e.g., *FTC v. VIZIO, Inc.*)
  - Poor cybersecurity practices (e.g., *FTC v. D-Link Corp.* and *LabMD v. FTC*)
- A key FTC decision focuses on failure "to take reasonable steps" to secure sensitive consumer information and found this failure "reasonably foreseeable"
- FTC has announced it will post weekly blogs to reinforce what is "reasonable"

But the Eleventh Circuit Potentially Dealt the FTC a Setback This Year in *LabMD*

- On June 6, the Eleventh Circuit overturned as unenforceable the FTC's cease-and-desist order in *LabMD*
  - The Court held that the order – which directed the company to "implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect" customer information – does not "enjoin a specific act or practice" and is thus insufficiently specific
  - This decision would appear to conflict with other cases in which similar FTC orders were enforced
- The implications of the order are uncertain now and will only become clearer over time:
  - Will the FTC seek rehearing *en banc* and/or cert?
  - Can the FTC address the decision by changing how it writes its orders or will it lead to wholesale enforcement changes?
  - Will the decision prompt any legislative action?

States – “Laboratories of Democracy”



States Have Increasingly Taken the Lead in Terms of Innovative and Cutting-Edge Data Privacy and Security Legislation

Data breach notification laws

- A wide range, with some states also imposing affirmative data security standards (e.g., MA and NY DFS)

Autonomous vehicle legislation

- 20+ states have passed legislation

Privacy laws

- A wide range of statues have been enacted
- California recently passed comprehensive privacy legislation
- 20+ states have passed social media privacy laws and close to half the states are considering laws on whether ISPs can collect customer data

Prime Example: *Facebook fails to evade suit alleging violations of Illinois biometric privacy law.* On the heels of losing a similar motion in a class action before the same judge, Facebook lost a motion to dismiss in a case involving claims that it stored scans of non-users' faces in violation of the Illinois Biometric Privacy Act (BIPA). BIPA restricts the use and storage of biometric data, including facial scans, and provides for a private right of action by consumers with fines up to $5,000 for each use of an individual's biometric data without their consent. Facebook moved to dismiss the suit arguing that the non-user plaintiffs had not alleged a concrete harm sufficient for legal standing, based on the recent Supreme Court ruling in *Spokeo v. Robins.* The judge rejected Facebook's motion to dismiss. The cases are *Gullen v. Facebook, Inc.*, No. 16-cv-00937 (N.D. Cal. 2018); and *In re FB Biometric Information Privacy Litigation*, No. 15-cv-03747 (N.D. Cal. 2018).

Data Laws: Security and Notification Statutes & Privacy

- Despite calls for action from some quarters, Congress has declined to enact a national data breach law—rather, federal data security and notification regimes are sector-specific
- All 50 states, D.C., Guam, VI and Puerto Rico, however, require data breach notification
  - Laws vary; some idiosyncrasies
  - Letters to affected individuals; some require reports to state Attorneys General
- Most relevantly here, a wide range of data breach notification laws, with some states also imposing affirmative data security standards (e.g., MA and NY DFS)
- State social media privacy laws
- State biometric laws (e.g., Illinois)
- The California Consumer Privacy Act and new causes of action related to data breaches (and a right to cure?)

Data Security and Notification Statutes (II)

Data breach obligations vary by jurisdiction and are ever changing. So it's always necessary to check. But key factors often include:

Covered Entities	• Some laws apply broadly to any entity conducting business in a jurisdiction, while others only apply to certain types of regulated entities.
Type of Information Implicated	• Jurisdictions differ in terms of what information must be implicated for notification to be required.
Definition of Breach	• Certain jurisdictions require unauthorized acquisition of customer information, while others require unauthorized access.
Risk of Harm Threshold	• When there is a breach, certain jurisdictions only require notification when there is a risk of harm.
Number of Residents Implicated	• The breach notification requirements can vary based on the number of a jurisdiction's residents that are implicated.
Existence of Safe Harbor	• Certain jurisdictions provide safe harbors from notification, such as when the information at issue is encrypted or notification is governed by another regulatory scheme, such as HIPAA.
Timing of Notice	• The timing requirements vary by jurisdiction, with some providing a specific deadline (which can be very short) and others standards.

The California Consumer Privacy Act of 2018 – Scope

Scope: Applies to "businesses … do[ing] business in the State of California" or businesses "that control[] or [are] controlled by" a business doing business in the state of California and that satisfy *one* of the following:

- have annual gross revenues in excess of $25 million;
- annually buy, sell, receive or share for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers or devices; or
- derive 50 percent or more of annual revenues from selling consumers' personal information.

Personal Information: Defined extremely broadly – i.e., to include "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" and "inferences drawn from any [personal information] … to create a profile about a consumer."

The California Consumer Privacy Act of 2018 – Obligations

- Broad privacy policy disclosure
- Give consumers a right to request personal information businesses have collected, shared, or sold, and to prevent businesses from selling consumers' personal information
- Allows consumers, with exceptions, to instruct businesses to delete their personal information altogether
- Allows consumers to prevent or "opt out" of the sale of personal information
- Prohibit businesses from selling personal information of individuals under the age of 16, absent consent
- Mandates that businesses cannot treat consumers differently based on exercising their rights, but would allow for incentives

The California Consumer Privacy Act of 2018 – Enforcement

- *Only* the Attorney General is allowed to bring an action against businesses for improperly selling, storing, or sharing personal information. Businesses have 30 days to "cure"
- Consumers are only allowed to bring a private right of action due to a security breach and are limited to statutory damages of $750 per consumer per incident
  - Consumers are also required to give businesses 30 days to cure before filing suit
  - Upon filing suit, consumers must also give the Attorney General notice of the suit
  - The Attorney General may decide to prosecute the action on its own, allow the consumers to proceed on their own, or instruct the consumers not to proceed
  - Consumers can nevertheless proceed with a suit claiming monetary damages

Other Key Trends

Privacy and Cybersecurity Litigation

Shareholders

- Securities fraud (alleged impact on stock price)
- Derivative actions (alleged breach of fiduciary duties of care or oversight regarding management of cyber risks or adequacy of public reporting)

Private Plaintiffs

- Tort law (e.g., negligence, invasion of privacy, etc.)
- Statutory
- Contract claims (e.g., customer agreement, privacy policy, etc.)
- Misrepresentation of practices

Business Parties

- Litigation not common; usually handled via negotiation
- Contract claims (e.g., compliance with law, security requirements, audit rights, notification, indemnification, etc.)

Litigation – Fiduciary Duties

Oversight of Business Risks

- Business judgment rule: so long as Board acts on an informed basis, in good faith, and without conflicts
  - Includes matters such as oversight over strategy, operations, and enterprise risk management

Oversight of Legal and Regulatory Compliance

- Board must assure itself that the company has established an information and reporting system reasonably designed to provide senior management and Board with timely and accurate information to permit an informed judgment about compliance with law
  - Once compliance systems are established, Board must monitor them
    - For example, by receiving periodic reports about its effectiveness and any issues that arise
  - Liability risk potentially arises if Board ignores "red flags" of material non-compliance or liability-creating events

Recent Cyber "Caremark" Suits

- *In re The Home Depot, Inc. S'holder Derivative Litig.* (N.D. Ga. Nov. 30, 2016)
- *Davis v. Steinhafel* (D. Minn. July 7, 2016)
- *Palkon v. Holmes* (D.N.J. Oct. 20, 2014)

Litigation – Data Breaches

Key Issue: *Is having personally identifiable information stolen, without anything else, sufficient to establish Article III standing after the Supreme Court's Spokeo decision?*

- Lower courts have tackled a number of cases in the wake of the Court's *Spokeo* decision (e.g., *Zappos* in CA9; *Attias v. CareFirst, Inc.* in CADC; *Kuhns v. Scottrade, Inc.* in CA 8; *Neiman Marcus* in CA7; *Michaels* in CA2)
- Splits are emerging, over whether harms have to occur to named plaintiff, over how to apply *Spokeo* to claims under various statutes (e.g., FCRA, TCPA, etc.), and, most importantly, whether identity theft alone is enough to establish standing
  - The Third, Sixth, Seventh, Ninth, Eleventh, D.C., and Federal Circuits say yes; but, the Second, Fourth, and Eighth Circuits generally say no
  - Compare *Neiman Marcus* and *Michaels*: Standing found in 7th Circuit; no standing in 2nd Circuit for a very similar credit card swiping hack

B2B Controversies – Topics and Trends

- Indemnification
- Limitations of Liability
- The impact of cyber liability insurance
- Data breach damages and risk allocations
- Representations linked to certifications and standards-setting bodies
- Clarifications of responsibilities (vendor managed, company managed)
- Rights of cooperation (for data breaches, data subject access requests)
- Audit rights
- EU GDPR Data Processing Agreements
- The privilege question (common interest/joint defense?)
- Accidental waiver? Audit/Compliance versus anticipation of litigation
- Cyber and data protection diligence and risk allocation in M&A

Evolving International Standards: GDPR and China

General Data Protection Regulation (went into force May 25, 2018)

- Comprehensive approach to privacy and cybersecurity across sectors
  - Applies to all data relating to an identifiable or identified person
  - Applies to businesses offering goods or services to individuals in the EU
- Substantial penalties – **up to 4% of global turnover (revenue)**
- Major cybersecurity features
  - Companies must have accountability and data protection officers
  - Companies must comply with information security and incident response requirements
  - Requires data breach reporting within 72 hours

China Cybersecurity Law

- State may establish "systems for cybersecurity monitoring, early warning, and notification"
- Foreign companies must complete at least four security audits by Chinese government agencies with unclear jurisdictions
  - Review criteria are unclear and there are concerns the process could be used to delay or block market access
  - Review focuses on "other risks that could harm national security," a vague phrase that fives the government authority to interpret the scope as broadly as needed
- Internet companies must assist public security organizations in protecting national security and investigating crimes (no definition or limitations on what this entails)

What the Future Holds

Data Privacy and Security in the Public Eye

Source: https://www.washingtonpost.com/

Big Issues on the U.S. Privacy Agenda

Challenges of AI, Machine Learning, Autonomous Decision-making	• AI will help us fight cyber threats more effectively via machine learning, but it will also be a more efficient attacker. • AI creates new privacy issues, including embedded biases, the de-anonymization of aggregate data, the collection of more data, the deeper analysis of data.
Social Media Reforms	• Facebook and other social media giants are addressing the spread of misinformation. How does data analysis play a role? What happens if they favor accounts or close accounts wrongly?
Encryption Exception for Government	• Trump has called for private corporations to provide encryption keys for government access.
Internet of Bodies (and Medical Devices)	• More medical data will be collected than ever, including whether and when you take medication and your reactions to it. • Should there be a duty to warn for companies that can track your data and catch health conditions you aren't aware of?
Smart Cities: Efficiency and Privacy	• In Smart Cities, urban areas will collect electronic data and supply information to manage assets and resources efficiently. • There will be consistent monitoring and huge data privacy concerns. When can the government access this data? Can companies? How do you opt out?

This program is for information only and does not constitute legal advice. The views expressed are the personal opinions of panelists/presenters and should not be attributed to anyone else, including their employers. This presentation does not create a lawyer-client relationship.

Beijing

Boston

Brussels

Century City

Chicago

Dallas

Geneva

Hong Kong

Houston

London

Los Angeles

Munich

New York

Palo Alto

San Francisco

Shanghai

Singapore

Sydney

Tokyo

Washington, D.C.

sidley.com