WILLKIE FARR & GALLAGHER LLP

PONDURANCE

NEW YORK WASHINGTON HOUSTON PALO ALTO SAN FRANCISCO CHICAGO PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

Dealing During COVID: Privacy and Cybersecurity Trends in M&A

Laura Jehl | Rick Borden | Doug Howard

May 25, 2021

Agenda

- Overview of Privacy and Cybersecurity Trends Facing Companies in the COVID and Post-COVID World
- Key Risks and Questions – And How To Think About Mitigation

Privacy and Cybersecurity Trends

- Cisco's 2020 Data Privacy Benchmark Study affirmed that privacy and cyber issues continue to be a significant priority for companies through the pandemic.
- The pandemic encouraged this prioritization by placing a spotlight on some key privacy and cyber issues.
- But adoption and enforcement of new laws (e.g., GDPR, CCPA, NYDFS) present a more permanent issue for companies, and COVID-19 has not stopped this trend.
- Brexit adds another layer of complexity, but draft adequacy decision should help
- More GDPR-like laws coming around the world – *see, e.g.*, Brazil – as countries seek adequacy decisions to continue to do business in Europe.
- Some chance for a federal law, but also expect robust enforcement of existing laws by Biden Admin regulators. (Presidential order and CMMC)
- *Schrems II* Decision Creates Significant Uncertainty Regarding E.U.-to-U.S. Data Transfers
- Don't forget about litigation…

Privacy Liability and Enforcement: Litigation Trends

- Recent notable settlements and fines highlight just how expensive data privacy and data security violations (or allegations thereof) can be.

Defendant	Settlement/Fine	Notes
Facebook	$650 Million	Largest settlement under Illinois BIPA
Equifax	$575 Million	Included massive injunctive reqs
Home Depot	~$200 Million	Still paying 6 years after breach.
Uber	$148 Million	Consumer class action still working through courts
Yahoo!	$85 Million	Does not include reduced enterprise value.
Capital One	$80 Million	Just the regulatory fine.

Sources –
Facebook: Tyler Hatmaker, "Facebook will pay $650 million to settle class action suit centered on Illinois privacy law", *TechCrunch*, https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/ (March 1, 2021).
Others: Dan Swinhoe, "The biggest data breach fines, penalties, and settlements so far", *CSO Online*, at https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html (March 5, 2021).

Privacy and Cybersecurity Forecast

- Expect More Litigation
  - Private right of action in CCPA for data breaches
  - Even for non-data breaches, plaintiff's lawyers continue to try to find creative ways to expand the private right-of-action by bringing actions involving—but not relying entirely on—CCPA; this is unlikely to stop anytime soon barring judicial intervention.
  - Illinois's Biometric Information Privacy Act provides meaningful statutory damages and attorneys' fees based on mere technical violations of the statute, no showing of harm

- Increased litigation activity presents increased risk that companies will have to produce information about privacy and security practices, intrusions, and breaches.
  - Companies should confirm that their practices match their public disclosures.
  - Companies should remain vigilant in their incident response efforts to preserve the attorney-client privilege over material generated as part of the response or remediation.
  - Where applicable, companies may want to consider alternative dispute resolution provisions in their privacy policies or service agreements (but see CCPA).

- And then there are the breaches: SolarWinds, Exchange, Colonial Pipeline…

What Does This Mean For M&A?

- Until recently, privacy/cyber diligence had been focused and limited
  - FTC/Regulator Attention
  - Sensitive Data
  - Security Breach Victim
- Changes in EU and US privacy law have raised the profile of and broadened the issues covered by privacy/cybersecurity diligence
  - Focus is broader than just PI
  - Detailed assessment of company's governance, compliance processes
  - Value of data/data as an asset
- Major breaches, and rise in frequency, size and cost of ransomware incidents have heightened concerns re: potential exposure.

Key Diligence Questions Today

- Key diligence questions that parties are asking today include:
  - Does the Company have an EU presence? Does GDPR apply? If so, does it have a strong compliance program?
  - Does the Company have a viable plan for CCPA/CPRA compliance? Does the Company have GDPR compliance processes to leverage?
  - Data Provenance – Has the data been collected and managed and identified in a way that permits the data to be used as intended?
  - Data Value – Have data assets been fully monetized?
  - Does Company have the right policies and practices in place?
  - Industry Specific Issues – Is the Company subject to sector-specific (or activity-specific) laws (NY DFS, NAIC, GLBA, HIPAA etc.)?
  - How sophisticated and effective are company's security measures?
  - Is the Company exposed to SolarWinds, Exchange, other breaches?

Agreements – General Privacy Reps

- Privacy and Data Security Schedule
  - Data protection and data security, including with respect to the collection, storage, transmission, transfer (including cross-border transfers), disclosure, destruction and use of Personal Identifiable Information
  - Taken commercially reasonable measures to ensure that Personal identifiable information is protected against loss, damage, and unauthorized access, use, modification, or other misuse, including any Personal Identifiable Information created, received, maintained or transmitted on behalf of the Company's or its Subsidiaries' customers
  - No prior knowledge of breach, security or privacy concern
  - Regularly tested for effectiveness of controls
- Robust privacy reps becoming the norm, even for deals where data is not central.

Agreements – Specific Privacy Reps

- Reps and other language designed to cover specific issues raised by specific laws like GDPR and other developments included more often.

"The execution, delivery and performance of this Agreement and any related agreements, or the consummation of the transactions contemplated hereby, will not cause, constitute, or result in a breach or violation of the Data Protection Requirements."

"There are no unsatisfied requests from individuals seeking to exercise their data protection rights under Data Protection Requirements (such as rights to access, rectify, or delete their Personal Data, or to restrict Processing of or object to Processing of Personal Data, or to data portability)."

"In respect of any Personal Data processed by the Company, the Company has made all necessary registrations and notifications of its particulars with the relevant governmental authority in accordance with the Data Protection Requirements."

Moving Forward…

- Review of Policies, Procedures and Operational Alignment
  - Complimentary technical due diligence to validate controls in broader view
  - Why is a SOC2 not sufficient?
- The market has yet to settle because the law is still unsettled.
  - CCPA Amendments just finalized in March, but CPRA on the way
  - New Virginia privacy law
  - Federal legislation?
  - Antitrust issues in data ownership, monetization and use?
  - EU's ePrivacy Regulation.
  - New privacy laws enacted or expected in countries around the world
- Trend line is clear — importance of data and cybersecurity issues in M&A increasing.

Your Presenters

Richard M. Borden
rborden@willkie.com
212 728 3872

Richard M. Borden is counsel in the Corporate & Financial Services Department and Cybersecurity and Privacy practice group where he focuses on intersecting areas such as technology transactions, cybersecurity and privacy risk management, Fintech and Insurtech.

Rick is at the forefront of cybersecurity and privacy issues, advising on big data governance and the Internet of Things, cybersecurity risk management, and technology sourcing and transactions. Rick translates the often-complicated language of technology, cybersecurity, privacy, risk and compliance to assure that it's understood from both a legal and business perspective. His experience on both the customer and vendor side of matters enables him to advise general counsel, C-Suite executives and boards of directors on how to understand potential risks and how to respond should they suffer an incident.

Laura E. Jehl
ljehl@willkie.com
202 303 1056

Laura E. Jehl is a partner in the Communications & Media Department and Co-Chair of the Cybersecurity & Privacy Practice Group. Focusing on the intersection of data, law and emerging technologies, Laura advises clients on a broad range of privacy and cybersecurity issues. She has extensive experience identifying and mitigating privacy and data protection issues arising out of the collection, use and storage of data as well as the design of new business models, products and technologies. A former senior in-house counsel and C-suite executive, Laura understands the business, legal and technological challenges and opportunities her clients face and helps develop innovative approaches to maximize the value of their data-based assets.

Doug Howard
doug.howard@pondurance.com
317 663 8694

Doug Howard is the CEO of Pondurance, a Managed Detection and Response (MDR) provider. Prior to Pondurance, he ran a $500M P&L with a team of 1000 experts across RSA Security's Global Services, internal IT, Security and Risk Management, as well as the Transformation Office for the $2.1B exit from Dell. Previously he was the founder of SAVANTURE, Inc., CEO of VBrick, Inc., President of USA.NET, Chief Strategy Officer of SilverSky, COO of BT Counterpane, and VP of Security and Business Continuity at AT&T Corp. Doug started his career in the US Air Force working under the direct command of the Joint Chiefs of Staff at the Pentagon. After the military, he moved into the private sector and held executive positions at Sprint, FLAG Telecom, Telenet and CSC.

PONDURANCE

WILLKIE FARR & GALLAGHER LLP