LATHAM & WATKINS LLP

Privacy+ Security Academy

24 May 2021

Data Security Law Workshop and Best Practice

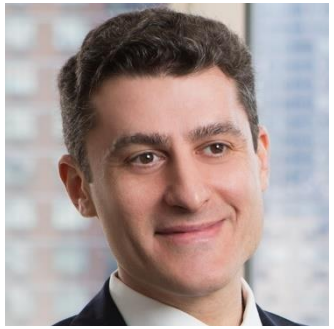
Jennifer Archie, Serrin Turner, Vincent D'Agostino, and Katie Clark

Speaking With You Today

Jennifer Archie

Connectivity, Privacy & Information

Latham & Watkins, Washington, D.C.



Serrin Turner

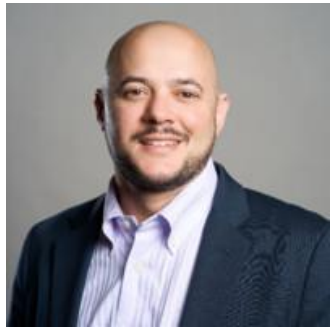
Connectivity, Privacy & Information

Latham & Watkins, New York

Fiona Maclean

Data & Technology Transactions

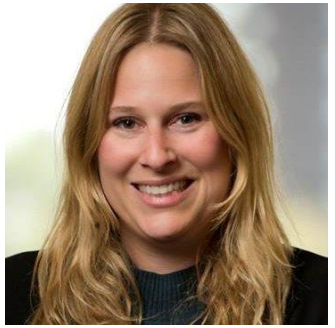
Latham & Watkins, London



Vincent D'Agostino

Head of Cyber Forensics & Incident Response

BlueVoyant



Katie Clark

Senior Vice President, Crisis & Reputation Risk

Edelman

Overview

1. **Incident Response** – aligning work-streams and experts to legal objectives and business outcomes

2. **Ransomware** – special legal and IR considerations

BREAK

3. **Attorney Client Privilege and Work Product Protections** — tips on managing contracting, report-writing, cases and controversies

4. **Round-up of Recent Data Security Legal Developments in US and Europe**

5. **Q&A + Close**

LATHAM & WATKINS LLP

Privacy+ Security Academy

Incident Response

Aligning Work-streams and Experts to Legal Objectives And Business Outcomes

Incident Response

The First 24 Hours

- Assembling the team
- Working together

Incident Response

Communicating Outside the Response Team

Employees

Law Enforcement

Affected Parties
(Commercial Partners)
commercial data or PII

Media

Investors / Shareholders

Regulators (Global / Regional Variations)

Affected Parties
(End Users, Consumers, Employees)
PII

Legislatures

Incident Response

Investigation/Fact Development

- The event – timeline, consequences, “attribution”
- Reasonableness of pre-breach security measures
- Sufficiency and timeliness of the post-event security enhancements

Incident Response

- Damage Assessment and Mitigating Harms to Affected Parties
- Managing Formal Legal Proceedings (quick trigger class actions or regulatory requests)
- Third Party Expert Reports

LATHAM & WATKINS LLP

Privacy + Security Academy

Ransomware

Special Legal and IR Considerations

Ransomware – Special Considerations

- Assembling The Team
- Contacts With Law Enforcement
- Whether To Pay, Consequences of Payments
- Communications Pressures And Challenges
- Mitigating Harms to Affected Parties
- Managing Formal Legal Proceedings
- Third Party Expert Reports

LATHAM & WATKINS LLP

Privacy+ Security Academy

BREAK

LATHAM & WATKINS LLP

Privacy + Security Academy

Attorney Client Privilege and Work Product Protections

Tensions and Tradeoffs

On the one hand…

- The privilege is important to protect sensitive discussions re potential liabilities / obligations
- Inaccurate or loose talk about security deficiencies can be seized on by adverse parties.
- Critical findings should be fully reviewed (including by Legal) before being finalized.

On the other hand…

- The protection offered by the privilege is limited.
- It may not be practical for attorneys to supervise every aspect of the response effort.
- The company needs documentation of its response effort that it can show to outside parties.

Materials Created by IR/IT Teams

Pre-Incident Materials

- Vulnerability scans
- Pen tests
- Red team exercises
- Risk assessments & audits
- Open security tasks
- Reports on prior security events
- Board briefings

Post-Incident Materials

- Response team IM communications
- Response team notes / analysis
- Forensic reports
- Discussions re remediation
- Post-mortem reviews

- These materials may be seized on by the other side to the extent they reflect any acknowledgment of a security deficiency.
- On the other hand, these materials may be useful to demonstrate a well-functioning security program.

Case Study: Target

- Target created a “Data Breach Task Force” to assist the company in its response to the breach.
- Target asserted Task Force “was not involved in an ordinary-course-of-business investigation,” but was formed to help counsel provide legal advice
- HOLDING: Task Force materials were privileged, because that team was **focused not on remediation** of the breach, but rather on **providing counsel information to use in rendering legal advice to** Target.

Case Study: Experian

- Court upheld privilege, finding **Mandiant report was prepared specifically to assist counsel**, even if that wasn't only purpose
  - Mandiant was hired by outside counsel
  - Counsel actually relied on report in preparing for litigation
  - Report was separate from prior Mandiant work for company
  - Report wasn't given to full IR team

Case Study: Premera

- Court rejected privilege, finding documents would have been prepared **regardless of any concern about litigation**, including:
  - (1) drafts of press releases and notices sent to customers (not containing attorney comments/edits)
  - (2) IT audits performed prior to breach
  - (3) root cause analysis of breach
  - (4) remediation timeline prepared by in-house counsel

Case Study: Dominion Dental Services

- Court found report was not privileged in part because **vendor's work was cited in customer communications about incident**
  - Reference to vendor made to reassure customers that competent investigation was underway
  - That is business purpose – undermines claim that report was primarily in anticipation of litigation

Case Study: Capital One

- Court rejected privilege, finding Mandiant's MSA predated security incident and its report likely **would have been generated regardless of litigation risk**
  - Capital One entered into MSA in part to "quickly respond to a cybersecurity incident should one occur"
  - Outside counsel agreement with Mandiant had same scope of work and payment terms as in MSA
  - Capital One designated Mandiant's fees as "Business Critical" expense, not "Legal" expense
  - Report was widely distributed – including 50 internal employees, Board of Directors, and outside accounting firm

Case Study: Clark Hill

- Court rejected privilege, finding “two-track investigation” theory to be a “story” with “little support in the record”
  - *Kovel* doctrine must be read narrowly, otherwise it would insulate many services from adversary process
  - True objective of forensic report was to obtain *consultant*’s advice, not legal advice
  - Distinguishes *Target* as case where
    - there was true two-track investigation
    - report was not widely shared
    - report was not focused on remediation

Best Practices

	Discoverable Materials	Privileged Materials
Purpose	Document preventative measures and response efforts	Assist counsel in protecting legal interests of company
Examples	• chronology of incident • facts about how the attack unfolded • steps taken to identify affected users • materials reflecting work done to contain and remediate breach • assessments/scans/inventories performed in the ordinary course	• assessments of fault or what went wrong • prescriptive statements (i.e., what the company should have done differently) • discussions re notification obligations • discussions re potential for harm • drafts of public communications • drafts of post-mortems
Best Practices	• assume materials will be discoverable • stick to the facts • do not assess fault or blame • do not draw premature conclusions • where in doubt, consult with counsel on whether privilege protocols apply	• keep counsel copied on communications • make clear you are acting at request of / to assist counsel where appropriate • mark materials “PRIVILEGED & CONFIDENTIAL” • mark any non-final document “DRAFT”

Best Practices

1. Coordinate with Legal to clearly define communications protocols and practices to be used during the response effort.
2. Train response personnel to assume communications and documents they create could be subject to outside scrutiny and used in litigation against the company.
3. Maintain notes and logs of response efforts that are purely factual (who did what when) and that are meant to be available to demonstrate response effort to outside parties.
4. Preserve the underlying data reviewed in the course of response effort.
5. Segment discussions of sensitive topics (e.g., root-cause analyses, lessons-learned reviews, public communications) and ensure counsel is consistently involved in these discussions
6. Post-mortem & lessons-learned docs (which will likely need to be produced) should be drafted under supervision of counsel.
7. Outside vendor must be engaged and supervised by counsel in order for privilege to apply to their work.
8. When communicating with or at direction of Legal, label those communications “PRIVILEGED & CONFIDENTIAL.” But do not overuse this designation – it can provide a false sense of security.

Special Waiver Considerations

Sharing Information with the Government

ETC…

Complete Waiver (Majority Rule)	Selective Waiver (Minority Rule)
Disclosure of privileged materials to government constitutes complete waiver over those materials, and that waiver applies in other matters.	Sharing privileged material with government under confidentiality agreement, does not waive privilege as to other entities or parties.

CISA
CYBER+INFRASTRUCTURE

No Waiver
"[T]he provision of cyber threat indicators and defensive measures to the Federal Government under this title shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection." CISA § 105(d)(1).

LATHAM & WATKINS LLP

Privacy + Security Academy

Round-up of Recent Data Security Legal Developments in US and Europe

Data Breach Litigation - Standing

Tsao v. Captiva MVP Restaurant Partners (11th Cir 2021)

- Recognizes circuit split
- No standing where cc#s stolen but no actual misuse
- Fact that data was targeted by hackers not sufficient to establish risk of ID theft

Steven v. Carlos Lopez & Associates (2d Cir 2021)

- Denies circuit split
- Actual misuse not required to establish standing
- Fact that data was targeted hackers strongly indicative of risk of ID theft

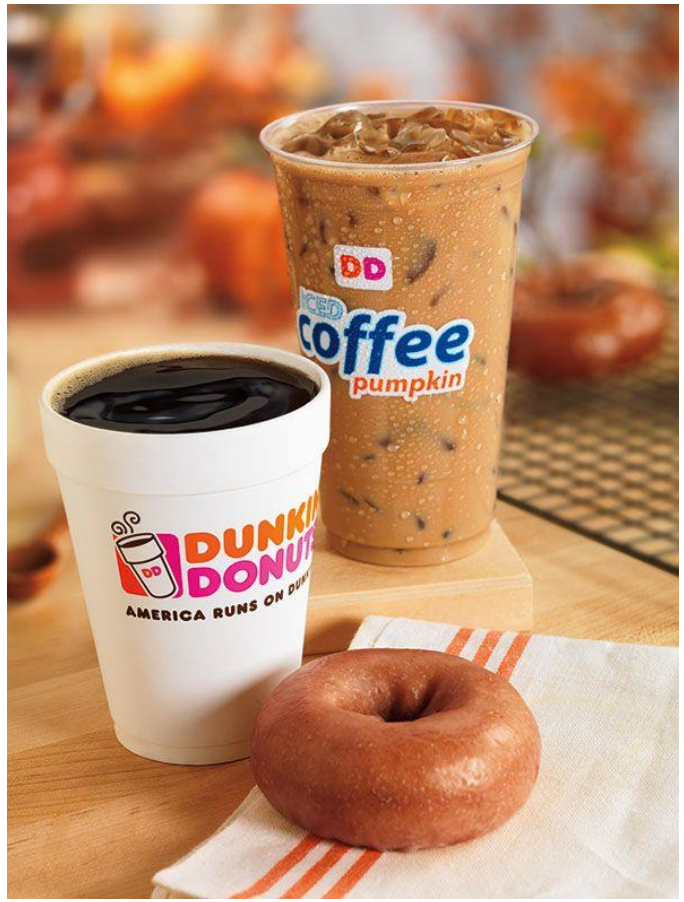
CCPA Litigation Developments

- *McCoy v. Alphabet* (Feb. 2, 2021)
  - CCPA cause of action only applies to data breaches
- *Gardiner v. Walmart* (Mar. 5, 2021)
  - CCPA's cause of action not retroactive to activity before Jan 2020
- *Maag v. U.S. Bank National Association* (Apr. 8, 2021)
  - Conclusory allegations of unreasonable security insufficient
- Still no case law yet on CCPA cure provision or statutory damages

FTC – Zoom Settlement

- FTC faults Zoom for deceptive security/encryption reps and circumventing browser security feature
- Chopra dissent critiques “unfortunate FTC formula” of “paperwork” remedies
  - Recommendations in dissent may be blueprint for future FTC enforcement strategies

NYAG – Dunkin Donuts



- Customer reward card accounts compromised through credential stuffing
  - Accounts connected to credit cards
- Dunkin Donuts faulted for failing to investigate incident or notify customers

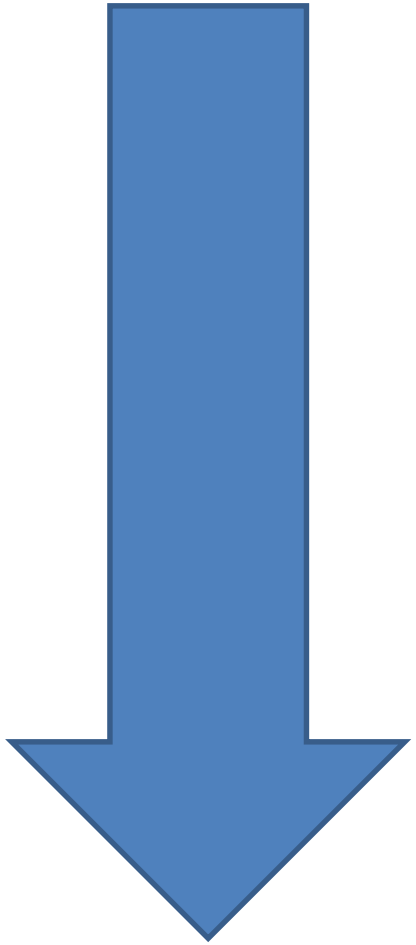
NYDFS – Residential Mortgage Services

- DFS exam uncovered email account compromise that had not been reported
- Account belonged to employee who handled customer PII on daily basis
- Company faulted for failing to look for PII in inbox and notify affected parties

EU/ UK General Trends

- General trend of increasing enforcement and increasingly large fines for privacy and security breaches continues across the EU and UK
- Security breaches made up approx. 20% of GDPR sanctions in 2020 (public source figures).
- Largest GDPR fines for security related issues so far are the ICO's BA and Marriott fines.
- Civil claims following data security breaches are becoming increasingly common (UK and across the EU).

The Biggest GDPR Fines of 2020-2021



1. Google - €50 million (France)
2. H&M - €35 million (Germany)
3. TIM - €27.8 million (Italy)
4. British Airways - €22 million (UK)
5. Marriott - €20.4 million (UK)
6. Wind - €17 million (Italy)
7. Notesbookbilliger.de - €10.4 million (Germany)
8. Vodafone Spain - €8.15 million
9. Google - €7 million (Sweden)
10. Caixabank - €6 million (Spain)

Class Actions/ Representative Actions

An increase in class actions (‘opt-in’) following data security breaches

Sector focus

UK Financial Service regulators are maintaining a focus on cyber and data security and resilience.

- **£56 million** fine issued by the FCA and the PRA against the RBS Group for inadequate testing procedures and failing to establish robust IT systems, which gave rise to consumer disruption as over 6.5 million customers could not access their accounts online for several weeks.

- **£16.4 million** issued by the FCA against Tesco Personal Finance plc in connection with a cyberattack, including for failure to take appropriate action to prevent the foreseeable risk of the cyberattack and failure to respond with sufficient rigour, skill and urgency

NIS Directive 2

- The NIS directive sets cyber and data security standards and incident notification requirements, across the EU and implemented in the UK. A proposal for a revised directive, NIS 2, was released in Dec 2020.

- The proposal expands the sectors and services within scope, to include electronic communications services, social media platforms, and data centre services. .

- The draft provides for maximum fines for certain breaches of the higher of EUR 10M or 2% annual global turnover (applicable to all in-scope providers/ operators), as well as for individual accountability for management in some cases.

LATHAM & WATKINS LLP

Privacy+ Security Academy

Questions?

Disclaimer

Although this presentation may provide information concerning potential legal issues, it is not a substitute for legal advice from qualified counsel. Any opinions or conclusions provided in this presentation shall not be ascribed to Latham & Watkins or any clients of the firm.

The presentation is not created or designed to address the unique facts or circumstances that may arise in any specific instance, and you should not and are not authorized to rely on this content as a source of legal advice and this seminar material does not create any attorney-client relationship between you and Latham & Watkins.