Armstrong Teasdale

Rising to the Challenge:

Anticipating and Responding to Creative Online Data-Related Claims

May 2018

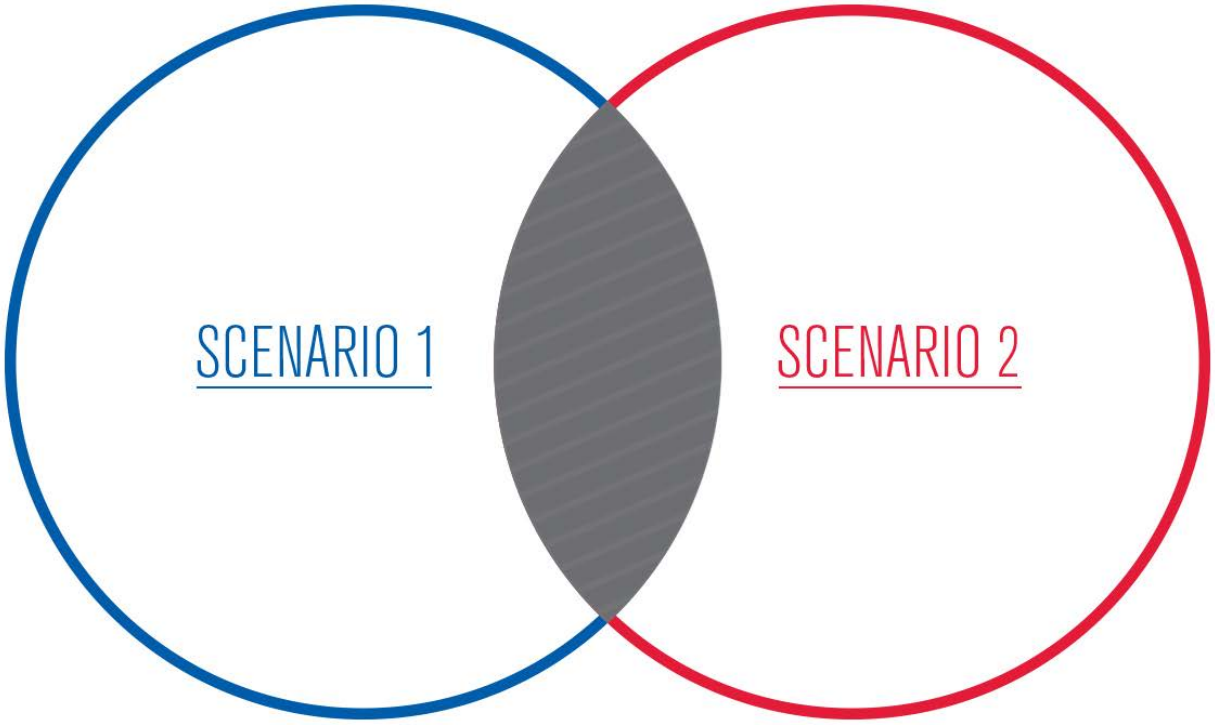
Jeffrey Schultz, CIPP/US

Agenda

- Common scenarios
- Incident response
- Legal actions to recover and protect data
- Creative claims arising from incidents

Common Scenarios

1. Company (data holder) did not intend to disclose the data
2. Company (data holder) intended to disclose the data
3. The gray area



Threats Giving Rise to Scenario 1: Malicious Conduct and Negligent Conduct

- **Insider:** departing employees; data saved on mobile storage devices; shadow IT (performance issues may encourage this behavior); lost devices; weak passwords; partnerships or programming that cause unintended consequences
- **Outsider/Insider:** social engineering ("hacking the wetware")
- **Outsider: Malicious hackers**
  - Recent attacks exploit RDP zero day flaws
  - Credential theft a big concern
  - Even VPN may not provide sufficient protection on compromised public WiFi (gap in coverage at login can expose login credentials and other valuable information)

Threats Giving Rise to Scenarios 2 and 3

- Lack of planning
- Unintended consequences
- Insufficient vetting or lack of control over third parties with whom data is shared

Data Breach Response

1. **Preparation**
   - Conduct a risk assessment, select a team, and develop a plan
2. **Identification and Declaration of an Incident**
   - Identify affected resources and potential impact on business
3. **Containment and Eradication**
   - Forensic investigation to confirm network resources affected, identify network “containment” points, and preserve logs and other evidence
4. **Recovery**
   - Technical (restoration of resources, etc.) and business (communications with constituents, etc.)
5. **Lessons Learned**
   - Institute a formal requirement for post-action review

Breach Response Note: Protecting Privilege

- **Attorney-client privilege/work product doctrine can be invoked between the victim company's outside legal counsel and hired third-party forensic firms that perform a review of the system during a breach. Allows the forensic company to report breach results directly to the law firm.**
- **Consider two-track approach to forensic investigation:**
  - One investigation at the direction of counsel to enable counsel to provide legal advice in anticipation of litigation.
  - A separate investigation by the business team to get things running again and/or report to any interested partners.

Breach Response (Generally): Emphasize Calculated Speed

- **Fight the tendency to wait for better information**
- **Faster communication of incomplete information generally preferred**
  - We have had a security event and are investigating…
- **Don’t over-promise in initial communications**
- **Centralize communications**

Taking Action: Strategies to Protect or Recover Information if You Know Who Took It

- **Cease and Desist letter?**
  - Pros: inexpensive; puts bad guy on notice of possible litigation and preservation obligations
  - Cons: bad guy may ignore; gives time to try covering tracks; delay harms chances of TRO
- **File an Action?**
  - Pros: shows you are serious; allows discovery
  - Cons: more expensive; may not have a lot of information at the time of filing
- **Seek a Temporary Restraining Order?**
  - Pros: obtain a court order prohibiting use and further disclosure; binding on those acting in concert with the bad guy who receive notice of order
  - Cons: much more expensive and a lot of up-front costs; often evidence against the bad guy is thin (present motion before any discovery)
- **DTSA ex parte seizure?**
  - Pros: ex parte; obtain control of information quickly
  - Cons: only in extraordinary circumstances; damages for wrongful seizure; very little case law

Claims to Recover and Protect Data

- Computer Tampering Statutes (some states and federal)
- Misappropriation of Trade Secrets (state and federal)
- Duty of Loyalty
- Fiduciary Duty
- Breach of Contract (ex: breach of an NDA)
- Tortious Interference
- Conspiracy (to pursue those acting in concert with the bad guy)

Practical Notes for Investigating Where the Data Went and Policing Compliance with Injunctions

- **Forensic imaging and review of devices before and during litigation**
  - Image and review company devices (if any) used by the bad guy
  - Seek an order allowing imaging and review of the bad guy's personal devices (*Ameriwood v. Liberman*)
- **Consider requesting the appointment of a monitor to assess the defendants' compliance with any injunction**

Legal Liability: Plaintiffs' Lawyers are Watching Closely and Exploring Creative Claims

Lots of victims in a data breach = class action!

Potential Claims Against the Data Holder (All 3 Scenarios)

- **Negligence**
  - Plaintiffs claim there was a duty to use reasonable care; protect and safeguard PII upon accepting and storing it
- **State Consumer Fraud Statutes**
  - Example: State Unfair and Deceptive Trade Practices Act (generally must have an ascertainable loss of money or property)
  - Plaintiffs allege that failure to comply with company privacy policy or to otherwise reasonably secure and protect consumers' data is an unfair and deceptive trade practice
- **Common Law Fraud**
  - Plaintiffs allege that failure to comply with a company's privacy policy or terms of use shows fraudulent misrepresentations

Potential Claims Against the Data Holder: *Continued*

- **Breach of Contract**
  - Failure to comply with privacy policies or terms of use
  - Indemnification and other contractual obligations owed to other companies or individuals
- **Breach of Fiduciary Duty**
  - Plaintiffs allege a special relationship creates a heightened duty (ex: if a healthcare provider suffers a breach of PHI)
- **Unjust Enrichment**
  - Alleges data holder was unjustly enriched because it saved money on security
  - Problem with theory: did plaintiff pay for the security?

Potential Claims Against the Data Holder: *Continued*

- **State Computer Tampering Statutes**
  - Plaintiffs allege that the defendant accessed or caused access to information without authorization or disclosed or took data without authorization
  - Tortured use of the statute against the data holder: it's aimed at providing an action against hackers who steal information, not the data holders from whom data was taken
- **Common Law Invasion of Privacy**
  - Must show that the defendant obtained information by unreasonable means
  - Difficult to apply against a data holder from whom the data was taken if the data was voluntarily given to the data holder

Other Attempted (and Creative) Claims under Scenarios 2 and 3: Wiretap Act

- **Website users have attempted to bring class actions for alleged "interception" of data without the users' consent**
  - Websites that use of cookies to gather data from users
  - Websites that use JavaScript intercept data from users
- **Big Risk to Company:**
  - Steep statutory fines and a lot of potential class members
- **Problems for Plaintiffs:**
  - The way the technologies operate doesn't fit within the statute
  - Party to the communication exception

Strategies Being Used by Plaintiffs' Lawyers

- File suit against smaller defendants first, then use settlements/consent orders to pursue bigger targets
- File in state courts with fewer resources; try to plead around CAFA
- Select rural venues
- Agree to settlement that provides for amendment, removal and nationwide class certification

Challenge for Plaintiffs: Standing/Injury in Fact

- **What level of harm must be inflicted on individuals whose information was affected by the breach to give them standing to assert a claim?**
  - ***Clapper***: The threat of injury must be certainly impending; allegations of possible future injury are not sufficient. Plaintiffs cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.
  - ***Spokeo***: "Injury in fact" requires that a plaintiff suffer an invasion of a legally protected interest that is concrete, particularized and actual or imminent, not conjectural or hypothetical.
- **Issue: How do plaintiffs allege damages/injury without any actual misuse of their information (i.e. there is not yet any actual harm, only a potential risk or increased risk of future harm)?**

Challenge for Plaintiffs: Standing/Injury in Fact

- **Circuit Split**
  - **Majority (D.C., Sixth, Seventh and Ninth Circuits)**: Data breaches create a substantial risk of identity theft; actual misuse is not required.
  - **Minority (Second, Fourth and Eighth Circuits)**: Such alleged future injuries are generally too speculative; there needs to be actual misuse of the data.
- **Plaintiff's burden of showing injury in fact increases as time passes (diminishes "imminence" of risk of harm):** Translates to a higher burden at summary judgment than at motion to dismiss and for claims filed long after the incident.

Challenge for Plaintiffs: Standing/Injury in Fact

- **Plaintiffs have tried to allege damages/injury in the form of:**
  - Unjust enrichment
    - Sharing data with others in exchange for money, services or other benefits
    - Avoiding expense of putting in place proper safeguards or properly coding a website; increase in defendant's business valuation
  - Loss of benefit of the bargain
    - Difficult to say that security was something bargained for in normal consumer transactions, especially when online charge is same as brick-and-mortar
  - Lost value of the data
    - Difficult because plaintiff needs to be able to show he/she desired to and could have sold the PII before it was improperly disclosed (need to establish there was a market for the data)
  - Statutory violation
    - Could potentially be used to try to avoid having to show injury-in-fact

Additional Defenses

- **Class Defenses**
  - Commonality/typicality issues: unique user settings, unique expectations, unique defenses
- **Appropriate Disclosures/Consent**
  - Privacy Policy
  - Terms of Use
  - Issue: clickwrap vs. browsewrap
- **Causation**

Bonus: ADA Claims Against Website Operators

- **Recent Trend**: Cease and desist letters to website operators alleging websites do not comply with ADA because screen reader technology (to convert text to audio) for the visually impaired won't work.
- Title III:
  - Applies if website operators are operating "a place of public accommodation."
  - 12 types of public accommodations, including catchall: "other sales or rental establishment." Conceivably covers most commercial establishments; doesn't expressly include websites.
  - Remedies available in private ADA suits: injunctions and attorneys' fees.
  - DOJ can seek civil fines and penalties.
- Title I:
  - Unlawful for an employer to discriminate against a qualified applicant or employee with a disability.
  - Employers must provide "reasonable accommodation" to enable applicants to be considered for a job.
  - NOTE: Some similar state statutes (CA) allow civil actions by the individual requesting the accommodation.
- How to Comply?
  - DOJ has hinted that websites should aim to conform to the Website Content Accessibility Guidelines (WCAG) 2.0, Levels A and AA.

Questions?

Jeffrey Schultz

CIPP/US, Partner at Armstrong Teasdale

314.259.4732

jschultz@armstrongteasdale.com

www.linkedin.com/in/jeffschultzesq

Armstrong Teasdale