UT LAW CLE | THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

2017 Essential Cybersecurity Law

July 28, 2017
Dallas, TX

Recent Trends and Developments in Cyber and Data Breach Litigation

Donald Houser
Daniel Felz

Recent Trends and Developments in Cyber and Data Breach Litigation
Donald Houser, Andrew Liebler, and Daniel Felz

I. Introduction

The explosion of cyber and data breach litigation has brought with it a host of issues for litigants and courts to wrestle with. This paper highlights some of the most important issues in cyber and data breach litigation today, with the goal of providing insightful overviews and key takeaways. Specifically, this paper covers:

- Standing under the Supreme Court's *Spokeo* decision and key takeaways on *Spokeo*'s application and importance.
- Standing under the Supreme Court's *Clapper* decision and key takeaways on *Clapper*'s application and importance.
- Emerging trends in cyber and data breach litigation, including financial institution litigation, developments in negligence claims, the economic loss rule, and offers of judgment.
- New cybersecurity and privacy liability risks companies may face from civil litigation or enforcement action under forthcoming E.U. privacy regulations.

II. The Right to Bring Claims in Federal Court and the Ever Changing Landscape of Article III Standing

Perhaps the most fundamental issue in cyber and data breach litigation is Article III standing because it serves as the Constitutional gatekeeper to bringing a lawsuit in federal court.[1] To have standing under Article III, a plaintiff must demonstrate, among other things, that they have suffered "injury in fact."[2] "To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete, particularized, and actual or

[1] For example, the search: "'Article III standing' and (invad! or invasion! /2 privacy) or (data breach)" results in over 5,000 federal cases in a legal research search engine.

[2] *See, e.g.*, *Lujan v. Def. of Wildlife*, 504 U.S. 555 (1992) (holding the injury must be more than merely "hypothetical").

imminent, not conjectural or hypothetical."[3] The focus on Article III standing in cyber and data breach litigation is driven by the attempts by both parties and courts to map this Constitutional (and jurisdictional) requirement onto new claims that, until recently, would have been unprecedented.[4] This friction point has produced two landmark Supreme Court decisions in the past four years – *Robins v. Spokeo, Inc.*[5] and *Clapper v. Amnesty International USA*.[6] The sections that follow provide overviews of the *Spokeo* and *Clapper* decisions, analyze how courts have wrestled with and applied these decisions, and conclude with a list of key trends and takeaways.

A. An Overview of the Supreme Court's *Spokeo* Decision

The Supreme Court granted certiorari in *Spokeo* to determine whether the bare violation of a statute – the Fair Credit Reporting Act ("FCRA") – is sufficient to confer Article III standing. The case arose when Plaintiff Thomas Robins alleged that Spokeo – a search engine operator that aggregates information on specific individuals from various public sources – had published false information about him. This false information included incorrect reports that Robins was married, in his fifties, had children, held a job, was relatively affluent, and had a graduate degree.[7]

---

[3] *Robins v. Spokeo, Inc.*, 136 S. Ct. 1540, 1548 (2016) (internal quotations and citations omitted).

[4] For instance, it would have been hard to image perhaps even a decade ago that headphones would be at the center of a class action lawsuit where plaintiffs allege that their headphones spied on them by tracking their listening history and selling that information without permission. *See Zak v. Bose Corp.*, No. 1:17-cv-02928 (N.D. Ill.). Even in the late 1990s most individuals did not own a cellular phone. *See* Wall Street Journal, Cellphone Ownership Soared Since 1998 (November 27, 2009) (reporting that the number of U.S. households with cellphones increased to 71% from 36% between 1998 and 2005). Thus, very few people could have envisioned a lawsuit arising out of allegations that a cellphone tracked the user's location, recorded keystrokes, and accessed call and browsing history. *See In re Carrier IQ, Inc., Consumer Privacy Litig.*, 856 F.Supp.2d 1332 (N.D. Cal. 2012).

[5] 136 S. Ct. 1540.

[6] 568 U.S. 398, 113 S. Ct. 1138 (2013).

[7] *Spokeo*, 136 S. Ct. at 1546.

Title search: Recent Trends and Developments in Cyber and Data Breach Litigation

Also available as part of the eCourse
2017 Essential Cybersecurity Law eConference

First appeared as part of the conference materials for the
2017 Essential Cybersecurity Law session
"Civil Litigation Update"