Simpson Thacher

Memorandum

Connecticut State Courts Address the Definition of "Injury" in the Data Breach Context

June 22, 2015

Introduction

Quantifying the degree of harm resulting from a data breach can be an inherently difficult task. Access to sensitive information can be appropriated but not exploited, data can be stolen but not distributed, and sometimes the digital trail goes cold before the fact of a breach can even be confirmed at all. Establishing an evidentiary threshold for harm at which notification requirements are triggered, therefore, can prove unwieldy. As a result, legislative and regulatory regimes generally require companies to mitigate against the possibility of harm by notifying potential victims before any harm is evidenced.[1]

The Connecticut courts were recently called upon to address whether a data breach constituted "personal injury" under a general liability insurance policy where there was no evidence that the stolen data had ever been accessed by a third party. Last month, the Connecticut Supreme Court affirmed an appellate court decision holding that a breach alone is not "personal injury" and, additionally, that triggering a notification statute is not a substitute for a personal injury. This holding will help to inform the ever more frequent discussions over what constitutes "injury" in the data breach context.

[1] The bulk of these requirements are contained in state statutes on the subject, the first of which is California's "Notice of Security Breach Act," which was enacted in 2002 (CAL. CIV. CODE § 1798.29 (2013)). Similar bills addressing notification have been proposed in Congress, most notably the Data Security and Breach Notification Act of 2015 (H.R.1770, 114th Cong. (2015); *see also*, *e.g.*, S. 1535, 112th Cong. (2011)), and President Obama expressed support for a federal law requiring companies to notify victims of breach in his 2015 State of the Union Address (The State of the Union Address (2015)).

Recall Total Information Management v. Federal Insurance Company[2]

A. The Facts

In 2003, IBM entered into a data record storage agreement with Recall Total Information Management, Inc. ("Recall"), which subcontracted with Executive Logistics, Inc. ("Executive Logistics") for transportation of those records. Four years into the contract, 130 data tapes fell out of one of Executive Logistics' vans near a highway exit and were taken by an unknown person.

The tapes contained employment-related data for over 500,000 past and present employees of IBM, including contact information, birthdates, and social security numbers. However, the tapes were not readable by a conventional computer and, though they were never recovered, there is no evidence that they were ever accessed after disappearing from the roadside.

IBM promptly notified the persons whose information was contained on the tapes and provided each with one year's worth of credit monitoring services. These efforts cost IBM $6 million, which was reimbursed by Recall after a short negotiation. Executive Logistics, which had general liability and umbrella insurance policies in place with Federal Insurance Company (the "Insurer") naming Recall as an additional insured, gave Recall a promissory note for $6 million and submitted a claim to the Insurer, which was denied. Recall and Executive Logistics filed suit against the Insurer in Connecticut Superior Court for the denial of coverage alleging, among other things, breach of contract based upon obligations of the Insurer under the policies to defend Recall and Executive Logistics against suits and to reimburse them for covered personal injuries. Though these policies had no explicit cybersecurity or data breach-related provisions and though they explicitly carved out losses relating to intangible property, Recall and Executive Logistics argued that the damages suffered in the wake of the breach fit within the general liability coverage in the policies.

B. The Court's Ruling

The trial court had granted summary judgment for the Insurer on three issues: (1) the Insurer had no duty to defend Executive Logistics because the policy only covered "suits," and the negotiations took place in the absence of such a suit, (2) the plaintiffs' losses were not covered under the property damage provision because the data was "intangible" property, which was carved out of the policy, and (3) the plaintiffs' losses were not covered under the personal injury provision of the policy because there had been "no injury to a person." After filing a failed motion for rehearing, the plaintiffs appealed to the Connecticut Appellate Court (the "Court"), which ultimately affirmed the trial court's grant of summary judgment. The Court's holding can be broken down into two sub-parts.[3] First, that the loss of the tapes did not constitute personal injury as

[2] *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 83 A.2d 664 (Conn. App. Ct. 2014), *aff'd per curiam*, SC 19291, 2015 WL 2371957 (Conn. May 26, 2015).

[3] With regard to the duty to defend, the Court held that, "[o]n the basis of a plain reading of the policy, we cannot conclude that the term 'suit' or phrase 'other dispute resolution proceeding' was meant to encompass the mere negotiations that took place in this case." (Recall at 671).

defined in the policy, and second, that triggering the remedial provisions of various state privacy laws did not constitute personal injury per se.

1. Publication as Injury

The plaintiffs argued that the loss of tapes fell within the policy's personal injury coverage because the policy's definition of personal injury included certain injury caused by the "publication of material that . . . violates a person's right to privacy." Plaintiffs based their argument on the definition of "publication" imported from the defamation context—roughly translating to "dissemination to a third party"—and sought to analogize their circumstances to "defamation per se" (in which actual injury does not typically need to be proven).[4] The Court rejected that analogy, declaring that, "[a]s the complaint and affidavits are entirely devoid of facts suggesting that the personal information actually was *accessed*, there has been no publication."

2. Notification Requirement as Injury

The second part of the Court's holding dealt specifically with the argument that, if per se harm did not result from the sort of publication at issue in this case, then the triggering of notice provisions of certain state statutes constitutes harm instead. Once again, the Court rejected the argument and found no evidence of harm:

> These notification statutes simply do not address or otherwise provide for compensation from identity theft or the increased risk thereof, they merely require notification to an affected person so that he may protect himself from potential harm. Accordingly, merely triggering a notification statute is not a substitute for a personal injury.

Taken with the holding on publication, the court's ruling on notification essentially closes the door on the argument that, absent evidence of actual harm or a statute explicitly foregoing such evidence, an injury has necessarily taken place as a result of a data breach alone.

Recall in the Context of the Current Legal Landscape

The opinion's treatment of what constitutes injury (and the concomitant requirement of access) supports the current jurisprudence on the necessity of injury in establishing standing in data breach cases. Specifically, as in other contexts, standing in a data breach case requires injury that is "concrete, particularized, and actual or imminent."[5] The Court in *Recall* was presented with the opportunity to lighten

[4] *See generally* Restatement (Second) of Torts § 570 (2013).

[5] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).

the burden on plaintiffs to show such injury by allowing them to use publication or the triggering of notification statutes as per se injury. By focusing on access in this particular factual circumstance, the Court rejects that opportunity in favor of consistency with existing case law addressing harm.

Indeed, this approach is the one used in the largest data breach cases of recent memory, both to confirm standing where identifiable harms exist[6] and to deny it where the harms are merely theoretical.[7] Without citing any of these cases or explicitly invoking the law of standing, the Court in *Recall* has required a showing of harm consistent with the existing case law that addresses data breaches in contexts other than insurance disputes.

Given that cybersecurity law is in its infancy, the landscape may shift. Companies should review their cybersecurity-related policies (insurance and otherwise) and engage counsel early in the event of any breach to ensure compliance with and utilization of the latest case law on the subject.

If you have any questions or would like additional information, please do not hesitate to contact any member of the Firm's Privacy and Cybersecurity Practice.

[6] *In re Target Corp. Customer Data Security Breach Litig.*, 2014 WL 7192478 (D. Minn. December 18, 2014).

[7] *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013).

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
1155 F Street, N.W.
Washington, D.C. 20004
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3919 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
West Tower, Mirae Asset Center 1
26 Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000