Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Peek Inside The New Data Privacy Lawsuit Playbook

Law360, New York (November 08, 2013, 7:11 PM ET) -- When a blogger revealed that Facebook tracked users even after they had logged off from Facebook's service, the company thanked him and promised an immediate fix. But plaintiffs' attorneys socked the company with a class action seeking $15 billion in damages for alleged privacy violations, a number just shy of what Facebook raised in its IPO.

Plaintiffs' lawyers are constantly searching for the next mega lawsuit, and data privacy looks very promising with its litigation trifecta: major consumer exposure, complex and increasingly antiquated state and federal data privacy laws, and ever larger and more frequent data breaches.

To the plaintiffs' bar, data privacy is starting to look like a high-stakes casino, and they're rolling the dice.

Plaintiffs' attorneys now frequently troll news reports and public records, sometimes filing class actions within 24 hours of a data breach. Their efforts to stay up to speed are aided by laws in almost every state that require companies that have experienced a breach to report themselves to customers, governmental authorities, or both. Thanks to mass-hacks — breaches on, in some cases, millions of customers' data — there is no shortage of victims. In 2012 alone, at leat 44 million records were compromised in 621 confirmed data breaches globally.

To share lessons and strategies learned from this fast-moving legal landscape, plaintiffs' lawyers recently held a conference in Philadelphia. Netflix's recent decision to settle a privacy class action provides a case study. Facing a damages demand that could have run into the billions of dollars, Netflix decided to settle the suit over its data storage practices for $9 million — including up to $2.25 million to plaintiffs' attorneys.

Plaintiffs' lawyers are adapting to the courts' historic skepticism toward data privacy suits by developing creative new legal theories. Their biggest challenge is overcoming the constitutional requirement that, to obtain standing in federal court, plaintiffs must show "an injury-in-fact" that is "concrete and particularized." Most courts have turned aside claims that allege data breaches injured plaintiffs by merely increasing their risk or fear of identity theft, or such claimed injuries as the cost of monitoring one's credit, emotional distress, or increased risk of junk mail, among others.

But new injury theories are gaining traction. One court found injury in data that contained a location tracking component because it overburdened the battery life of the plaintiffs' smart phones.

And a recent California ballot initiative would have amended the state constitution to create a presumption of harm to individuals whose personal information was disclosed without consent. The

initiative was abandoned after the Legislative Analyst's Office determined it could spur "unknown but potentially significant costs" from lawsuits. Among other things, it would have resulted in a field day for the plaintiffs' bar and exposed practically every entity doing business in California to class actions.

Meanwhile, in an effort to evade the injury requirement entirely, plaintiffs have begun gravitating to federal and state laws containing so-called statutory damages provisions. Federal statutes such as the Electronic Communications Privacy Act (ECPA) (which includes the Stored Communications Act and the Wiretap Act) and the Video Privacy Protection Act, along with many state laws, set forth statutory damages for each violation. These laws specify damage awards rather than allowing courts to calculate damages based on the degree of actual harm to the plaintiff. Indeed, these laws require no evidence of actual injury at all.

Plaintiffs' lawyers also benefit from state laws that effectively require companies victimized by data breaches to sound an alarm bell, sending the attorneys down the fireman's pole and off to the courthouse. For instance, 46 states have data security statutes requiring notification of breaches, and about a dozen provide a right to sue to consumers and others who claim they were harmed. Of the roughly 20 federal statutes that regulate privacy broadly, 13 contain a right to sue.

These statutes vary as to what events trigger notice to consumers, what exceptions to these triggers the states recognize, and whom the corporate breach victim must notify and who may enforce (e.g., attorney general or individuals, or both).

For example, Massachusetts' notification law is triggered by either the unauthorized acquisition or misuse of personal information, or a substantial risk of identity theft or fraud. In Florida, unauthorized acquisition of personal data alone requires notification. All states with breach notification laws require that the breached company notify the individuals affected, but some also require that the state attorney general be notified.

This hodgepodge of breach notification laws creates uncertainty for consumers and for businesses that collect users' personally identifiable information. And this is fertile ground for the plaintiffs' bar.

Streamlining and modernizing our laws is the first step to protecting both consumers and corporations. That is why the U.S. Chamber of Commerce supports a uniform federal standard for breach notification that is consistent with the best approaches in state law. The legislation also should contain carefully drafted provisions addressing preemption, liability and enforcement.

To be sure, no business wants to expose its customers to data privacy pirates. But as companies constantly work to keep one step ahead of the bad guys, the goal should be to achieve real data security with legal clarity, rather than another big payday for the plaintiffs' bar.

—By Robert M. McKenna, Orrick Herrington & Sutcliffe LLP, and Lisa A. Rickard, U.S. Chamber of Commerce

Robert McKenna is the former attorney general of the state of Washington and the current co-head of Orrick Herrington & Sutcliffe's Public Policy Group. Lisa Rickard is president of the U.S. Chamber's Institute for Legal Reform.