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

Top Privacy Cases Of 2015: Midyear Report

By **Emily Field**

Law360, New York (June 30, 2015, 3:38 PM ET) -- The U.S. Supreme Court ruled that social media posts aren't threats without intent and strengthened protections of corporate data records, while a retail tracking firm's settlement with regulators has attorneys on the lookout for a rise in consumer class actions. Here, Law360 examines the most important privacy decisions and settlements of the year thus far.

U.S. v. Elonis

Earlier this month, the Supreme Court ruled that online posts can't be considered threatening if that wasn't the author's intent when it struck down the conviction of a man who had made violent Facebook posts about his wife, law enforcement officials and others.

The high court, in a 7-2 decision, reversed the Third Circuit's 2013 ruling that held that the test for determining whether a statement falls under the First Amendment's "true threat" exemption depends on how a reasonable observer would view the message. Instead, the high court ruled that the test hinges on if the author meant the posts to be threatening.

The justices vacated the conviction of defendant and petitioner Anthony Elonis, who in multiple Facebook posts discussed killing his wife with a mortar launcher and blowing up FBI agents. However, the Supreme Court did send the case back to the lower court to give prosecutors a chance to retry the case on the intent standard.

However, the court's narrow decision, while holding that a speaker's intent behind a statement determines whether it is a threat or not, still left open questions, such as how lower courts should assess intent.

"The court's disposition of this case is certain to cause confusion and serious problems," Justice Samuel Alito wrote in his dissent. "The court holds that the jury instructions in this case were defective because they required only negligence in conveying a threat. But the court refuses to explain what type of intent was necessary."

Andrew Serwin, a partner with Morrison & Foerster LLP, said that the decision shows that it can be hard to predict how courts will decide in emerging areas such as social media.

"We're going to continue to struggle where these lines get drawn with social media and how courts are going to react," Serwin said.

City of Los Angeles v. Patel

Last week, the high court **struck down** a Los Angeles law that enabled law enforcement officers to drop in without warning at hotels and motels to inspect guest registries at any time, without a warrant or a subpoena.

The ruling — one of several in recent years that sided with privacy advocates over law enforcement — boosted companies' ability to protect customer data from government searches.

In a 5-4 decision written by Justice Sonia Sotomayor, the Supreme Court said that only a small number of industries intrinsically dangerous to the public are subject to a warrantless examination of their business records, upholding a Ninth Circuit decision that struck down the law.

Under the city's law, hotel owners could have been arrested on the spot if they refused a search.

The ruling means that businesses will be better able to protect their customers' information from government searches, according to Eric Miller, a partner with Perkins Coie LLP.

The Supreme Court held that a hotel owner must have the opportunity for judicial review of an officer's demand to search the registry before facing penalties for not complying.

Sotomayor noted that only four industries — car junkyards, liquor sales, gun sales and mining — have been identified by the high court as being so regulated by government that there's no reasonable expectation of privacy for them.

Scott Vernick, a partner with Fox Rothschild LLP, said that the high court's decision may indicate how courts will react to surveillance issues in a national security context.

"[The decision] does send a signal that a court that is sometimes considered conservative by many is not just rubber-stamping these warrantless requests," Vernick said.

Federal Trade Commission v. Nomi Technologies

The Federal Trade Commission's **first ever action** in the new mobile retail tracking industry sent a signal that the agency is keeping a close watch on how companies are living up to their privacy policies, no matter how new their technology is.

In April, Nomi Technologies agreed to settle FTC allegations that the firm deceived customers by not following through on a promise to provide them with a way to avoid being tracked.

The company's privacy policy stated, starting in 2012, that an opt-out mechanism would be available and that consumers would be informed when a retail store was using the tracking service, according to the FTC.

But Nomi, which has collected information from millions of customers' mobile devices, never delivered on those promises, the regulator said.

Data that provides an insight into customers' shopping and buying habits is extremely valuable to retailers. Nomi places sensors in its clients' retail stores that collect the unique 12-digit identifiers on customers phones while the devices search for WiFi networks, according to the FTC.

Nomi's privacy policy stated that, beginning in 2012, an opt-out mechanism would be available and that consumers would be informed when a retail store was using the tracking service, the FTC said. But the firm, which has collected information from millions of customers' mobile devices, never lived up to its end of the privacy policy, the regulator said.

"The technology is becoming increasingly popular as brick-and-mortar stores strive to

compete with e-commerce," said David Almeida of Sheppard Mullin Richter & Hampton LLP.

"Plaintiffs privacy lawyers are likely to take note of this FTC action (a first of its kind against beacon technology) because it brings a new type of technology into the crosshairs of a common plaintiffs' theory in privacy actions — namely, the collection and/or disclosure of consumer data without permission or in such a manner that exceeds the scope of permission," Almeida said.

However, these types of privacy class actions often fail because proving actual harm is generally difficult, Almeida said.

"But given the recent FTC scrutiny, we are closely monitoring how the plaintiffs bar reacts," Almeida added.

RadioShack Consumer Data Deal

After intense scrutiny from state regulators, the FTC and other companies, RadioShack Corp. **got interim approval earlier** in June for an agreement that will protect customers of Verizon and AT&T Wireless in a $26 million sale of data and intellectual property as part of the fallen retailer's bankruptcy.

In the deal, the data of the two phone companies' customers will be kept quarantined from General Wireless, the company that scooped up the assets along with 1,700 of RadioShack's store locations.

The data will be collected, scrubbed of any barred info and then moved to General Wireless, according to court papers. It appears the company will be able to identify the relevant data by isolating batches of bar code numbers connected to the companies and holding back those transactions from the data pool.

Under another privacy-related deal forged in May during a daylong mediation session in Dallas, the amount of information available to the buyer was whittled down from up to 170 data points to seven per customer record, and will not include credit or debit card information, Social Security numbers, telephone contact information, or dates of birth.

RadioShack filed for Chapter 11 protection in February, listing $1.4 billion in debt and becoming the latest high-profile casualty of consumers' shift away from brick-and-mortar retail.

Dozens of states' attorneys general had objected to the inclusion of customer data as part of RadioShack's bankruptcy offerings, pointing out that the defunct electronics retailer's database included nearly 40 percent of the country's population.

While the transfer of customer data in a bankruptcy or a merger is not a new issue, the deal highlighted the need for companies to be transparent and consistent in their privacy policies, including informing consumers that their data might be sold in the event of a bankruptcy or merger, according to Vernick.

"That's where [companies] have gotten tripped up, if they're inconsistent, or they buried the clause saying they'll [sell data if the company is sold]," Vernick said. "Everybody is very mindful of the need to be as transparent as possible."

Recall Total Information Management Inc. et al. v. Federal Insurance Co. et al.

Last month, the Connecticut Supreme Court was the first state high court to rule on data breach coverage under traditional general liability policies, when it affirmed a decision

nixing coverage for the $6 million in losses IBM Corp. incurred in dealing with a 2007 highway mishap that exposed the sensitive information of 500,000 employees.

The case had become a focal point in the data breach coverage debate after Sony Corp. settled its feud with insurers over coverage for the infamous PlayStation Network cyberattacks before a New York appellate court could rule on Sony's appeal.

The Connecticut Supreme Court, adopting the decision of a midlevel appeals court, held that a pair of insurers didn't have to cover losses tied to an incident in which a cart holding IBM computer tapes fell out of the back of a transportation contractor's van near a highway exit ramp. About 130 of the tapes, which contained Social Security numbers, birth dates and contact information for past and present IBM employees, were taken from the road by an unknown person.

According to the opinion, IBM contractor Recall Total Information Management Inc., now known as Recall Holdings Ltd., and subcontractor Executive Logistics Inc. had not triggered a section of the relevant policy providing coverage for injuries caused through the publication of material that violates a person's right to privacy.

Some policyholder attorneys have asserted that the decision will have limited application because of the unusual facts of the case, arguing there’s no evidence that anyone accessed the information, unlike in a typical data breach case.

Wiley Rein LLP partner Laura Foggan, who heads the firm's insurance appellate group, however, said the decision is "not actually a limited ruling," as "we commonly have the kind of factual setting that the case represents."

"What happens when an encrypted laptop is lost at the airport, or a mobile phone is left in a restaurant?" Foggan said. "These are common occurrences and similar to the issues in Recall Total. I think the impact at the end of the day will be very substantial and broad."

--Additional reporting by Allison Grande, Jeff Sistrunk and Cara Salvatore. Editing by Kat Laskowski.

All Content © 2003-2015, Portfolio Media, Inc.