

RadioShack Bankruptcy To Test Shelf Life Of Privacy Vows

By **Allison Grande**

Law360, New York (April 03, 2015, 8:58 PM ET) -- With state regulators raising objections to RadioShack Corp.'s potential sale of personal data of up to 117 million customers, the company's bankruptcy proceedings will test whether privacy promises made to customers live on after a business has collapsed.

In an objection filed in the Delaware bankruptcy court proceedings on March 23, Texas Attorney General Ken Paxton argued that selling the customer information database would flout not only RadioShack's own privacy policies, but consumer protection laws in Texas and other states. The database contains information on nearly 40 percent of the country's population, the attorney general pointed out.

The contention has since been backed by dozens of other state regulators, including New York Attorney General Eric T. Schneiderman, who recently announced that his office was monitoring the bankruptcy sale. Companies that collect private customer data on the condition that it will not be resold have the responsibility to "uphold their end of the bargain," Schneiderman said.

"When a company obtains customer personal information in return for a pledge not to sell it, the [Federal Trade Commission and other regulators] can enforce that agreement against the company," McCarter & English LLP partner Scott Christie told Law360 Friday. "However, in a bankruptcy situation, the company that made the pledge may cease to exist, and the temptation is to maximize value for shareholders and creditors."

By raising their objections, the state attorneys general have brought to center stage the issue of how broadly representations made to consumers about what companies will and won't do with their data can be applied, and whether a change in corporate ownership can diminish those promises, attorneys say.

On the one hand, the state regulators and other data protection authorities could argue that a broad promise to not sell customer data to third parties, such as the one that RadioShack made to its customers, can be interpreted to extend to any sale, whether or not the company is still in the form it was when the pledge was made.

"The involvement [of state attorneys general] reflects that the integrity of customer personal information collected by companies in return for a promise not to sell that information will be protected even where the company that made the promise no longer exists," Christie said. "Companies involved in bankruptcies and mergers should not expect to be relieved of their obligation to protect the privacy of

customer personal information."

But on the other hand, RadioShack could counter that the promise it had made applied only to its activities while in operation, and not to sales necessitated by either a bankruptcy or a merger, attorneys noted.

"The idea in privacy policies that you aren't going to sell data usually means you aren't selling it to third parties like data brokers without telling the customer," Fox Rothschild LLP privacy and data security practice leader Scott Vernick said. "Outward-facing privacy policies to consumers were never designed to prevent the transfer of data if a company had to sell all of its assets. That's not what the policies were designed to protect."

The fight over RadioShack's ability to hand off the massive customer database was put on hold Tuesday, when the bankruptcy judge overseeing the case approved a proposed sale offer from Standard General LLP that left the contested data assets out of the equation for now.

But the customer information is likely to come back into play later in the proceedings, highlighting how important it is for companies to make sure their representations to customers about what data they are collecting and what they are doing with it are clear.

"It is imperative for businesses to consider these issues at the outset," said Lisa Sotto, the head of Hunton & Williams LLP's global privacy and data security practice. "Companies that collect personal information pursuant to a privacy policy that severely restricts disclosure of the data and does not account for data sharing in bankruptcy are playing Russian roulette."

According to Sotto, an "easy fix" for companies would be to consider the possibility of bankruptcy at the start when crafting a privacy policy, so that if the issue does arise, it will be clear what the company can and can't do with its valuable customer data assets.

"It is foolhardy not to do so," Sotto added.

The dispute over the sale of customer data in bankruptcy auctions is not without precedent.

Borders Group Inc. faced scrutiny from the FTC and 24 state attorneys general in 2011 over its plan to sell its intellectual property — including its database containing the personal information of about 48 million customers — to rival Barnes & Noble Inc.

The deal eventually won approval from a New York bankruptcy court judge, after the FTC backed down and the parties made concessions such as publishing ads to inform the public of the sale and giving customers 15 days to opt out of having their data transferred in order to ease the privacy concerns.

However, the FTC took a more aggressive stance with bankrupt online toy store Toysmart.com LLC, which the commission sued in July 2000 for allegedly violating Section 5 of the FTC Act by attempting to sell customers' personal information despite its privacy policy stating that this information would never be shared with third parties.

Toysmart penned a settlement with the FTC later that month that prohibited the company from selling the customer list as a stand-alone asset. The deal stipulated that the company would be allowed to sell this information only to a "qualified buyer" — which was defined as an entity in a related market that

agreed to abide by the terms of Toysmart's privacy statement — as part of a package deal that included the entire website.

So RadioShack's case is just the latest in a string of reminders that companies should make sure a bankruptcy scenario is explicitly mentioned in any privacy policy that could later be scrutinized by federal or state regulators.

"What may happen now is that these policies would be reworded more carefully in light of the concerns expressed by the regulators in the RadioShack proceedings to say there may be an exception to a promise not to sell customer data for the sale of the company or all or essentially all of its assets," Vernick said.

And given that federal and state regulators are becoming increasingly active in enforcing privacy and data security issues that have a direct impact on consumers, a failure to clarify outward-facing statements may result in companies finding themselves in the same situation as RadioShack down the road, according to attorneys.

"Customer personal information is a valuable company asset," Christie said. "The scrutiny of Radio Shack demonstrates that state attorneys general will seek to intervene in bankruptcy proceedings to preserve the protection of customer personal information when enforcement against the company would be challenging if not impossible."

RadioShack is represented in the bankruptcy proceedings by David G. Heiman, Gregory M. Gordon, Thomas A. Howley and Paul M. Green of Jones Day, and David M. Fournier, Evelyn J. Meltzer and John H. Schanne II of Pepper Hamilton LLP.

The case is In re: RadioShack Corp., case number 1:15-bk-10197, in the U.S. Bankruptcy Court for the District of Delaware.

--Editing by Kat Laskowski and Katherine Rautenberg.