October 29, 2013

FTC Power to Patrol Unfairness in Privacy, Data Security Challenged, But Enforcement Push Likely to Continue

by Katie W. Johnson, Alexei Alexis and Donald G. Aplin

Even as the Federal Trade Commission seems poised to extend its power to regulate privacy and data security under Section 5 of the FTC Act, a ruling in a pending federal court case could curtail that power, privacy scholars and attorneys have told Bloomberg BNA.

The FTC historically has brought its privacy cases under Section 5 of the FTC Act, 15 U.S.C. § 45, which allows the commission to prevent "unfair or deceptive acts or practices in or affecting commerce."

"FTC privacy and security enforcement began with merely enforcing broken promises that companies made," according to Daniel J. Solove, the John Marshall Harlan research professor of law at George Washington University Law School, and Woodrow Hartzog, assistant professor at Samford University Cumberland School of Law.

"But in the past 5-10 years, the FTC has developed a much more robust and expansive enforcement approach, including a substantive body of baseline regulatory requirements. Expect the FTC to continue on this trajectory."

"The FTC seems poised to move beyond the four corners of a company's privacy policy and take a holistic view about whether a company adequately protects consumers through things like design decisions and training programs," Solove and Hartzog added.

Use of Unfairness Prong Questioned

Some have argued that the FTC has gone too far in flexing its enforcement muscles, especially in the context of regulating the data security practices of companies under Section 5's unfairness prong.

In the "not too recent past," FTC commissioners and others stated that the commission had no unfairness authority to regulate data privacy because there is no cognizable harm, noted Alan L. Friel, a partner at Edwards Wildman Palmer LLP in Los Angeles.

And in a data-breach enforcement action pending in the U.S. District Court for the District of New Jersey, hotel company Wyndham Worldwide Corp. has challenged the FTC's ability to regulate corporate data security under that unfairness prong (12 PVLR 1465, 9/2/13).

Even if the FTC has authority, the defendants added, it failed to provide fair notice through regulations or guidance as to what Section 5 requires concerning data security.
A hearing on the motions to dismiss is scheduled for Nov. 7.

More Rulemaking Authority?

If the court rules against the FTC in the Wyndham case, "there will be increased pressure for Congress to grant the FTC rulemaking authority," Solove and Hartzog said.

Berin Szoka, president and founder of technology advocacy group TechFreedom, said that if the court "rules that the FTC's approach in this area has failed to give the FTC 'fair notice' of what constitutes 'reasonable' data security, the FTC will, of course, declare an emergency and insist that Congress fill a perceived legal vacuum."

"The FTC should be given the ability to promulgate privacy regulations," Susan Grant, director of consumer protection at the Consumer Federation of America, said. She identified the White House's white paper calling for a "Consumer Privacy Bill of Rights" (11 PVLR 355, 2/27/12) as "the perfect vehicle" for providing that power to the FTC. Under that proposal, the commission would, for the first time, be able to prescribe formal rules giving consumers control over how their personal information is handled across various U.S. sectors. But the White House effort "seems only illusory at this point," she said.

Data breach notification is the area where the FTC will most likely obtain new rulemaking authority, said Szoka. But Grant said she would be "wary" of giving the FTC regulatory power in this area "as the states are already way out front on that and I would not want to preempt their laws with a federal law that might be weaker."

Legislative Prospects

Congressional Republicans have been hesitant to grant the FTC rulemaking authority, citing the potential for burdensome regulations. Industry groups have tried to make the case that existing statutes, such as the FTC Act, and industry self-regulation have been effective in protecting the privacy of U.S. consumers and that unnecessary regulations could do more harm than good.
And while there has been broad consensus in Congress and among stakeholder groups about the need for legislation focused on data security in the wake of high-profile breaches, conflicts over details such as the scope of covered information have hindered final passage.

Bart Lazar, a partner at Seyfarth Shaw LLP, in Chicago, said that a loss for the FTC in the Wyndham case might bolster efforts to push a data security bill over the finish line, after years of failed attempts. "There is definitely a need for this already because of differing requirements at the state level," Lazar said.

Lisa Sotto, a partner at Hunton & Williams LLP, in New York, said that a commission defeat would leave an immediate void in the area of data security oversight and enforcement. "That void would not last long," she predicted. "If the FTC loses its ability to enforce data security rules, it is difficult to imagine that Congress would not quickly step in to reinstate the FTC's authority—and possibly enhance it."

However, Alysa Zeltzer Hutnik, a partner at Kelley Drye & Warren LLP, in Washington, was skeptical about the possibility of the case triggering new federal standards, especially in the short term. "Year after year, there have been unsuccessful efforts to get Congress to pass privacy legislation," she said.

Whether the FTC wins or loses at the district court level, Hutnik said there will almost certainly be an appellate track in the case. In addition, she said there are dim prospects for legislative action in the near future, given that an election year is coming up and lawmakers have been unable to reach agreement on many issues lately.

Consent Orders as Common Law?

Even in the absence of direct congressional action, privacy scholars say the FTC will continue to rely on negotiated consent orders to establish the commission's rule of law.

In their forthcoming paper "The FTC and the New Common Law of Privacy," Solove and Hartzog say that the FTC's privacy jurisprudence—specifically, its settlement agreements with companies—is similar to a body of common law.

"There is no common law based on FTC decisions," Friel of Edwards Wildman Palmer said. Consent orders demonstrate what actions the FTC thinks are inappropriate, but they are "neither a basis for something having been illegal nor for remedies for what the law requires," he said. But enforcement actions are "really how the FTC has governed privacy and data security," TechFreedom's Szoka pointed out. The argument that the FTC's settlements are equivalent to a body of common law "raises deep problems about the rule of law," he said.

The FTC is "trying to bring all the major players in the tech ecosystem under consent decrees so it can enforce those directly, making enforcement even easier and allowing the FTC to impose a monetary penalty—without Congress having to give the agency general civil penalty authority for first-time violations of Section 5," Szoka added. He pointed to Google Inc.'s agreement to pay a $22.5 million penalty for its alleged circumvention of browser privacy settings as an example (11 PVLR 1255, 8/13/12).

Solove and Hartzog, meanwhile, said that the commission "hasn't overstepped its boundaries because its Section 5 authority is quite substantial." The terms in that section—"unfair" and "deceptive" practices—are "very broad," they said.

"The FTC has been quite consistent and conservative in its enforcement, and it has targeted companies whose practices stray far from the norm," Solove and Hartzog said. "We believe the FTC has the power to be much more potent in its enforcement than it has been."

Enforcement Areas to Watch

The FTC's data security and privacy enforcement efforts will likely focus on:

• Children's Privacy: In the beginning of 2014, companies should expect to see a "flurry" of Children's Online Privacy Protection Act civil investigative demands related to the amended COPPA Rule, with a likely focus on the use of persistent identifiers and mobile devices, D. Reed Freeman Jr., a partner at Morrison & Foerster LLP in Washington, said.
• Internet of Things: Szoka said to expect more enforcement actions concerning the "Internet of things," or the ability of consumer devices to communicate with other devices and people.
• Security by Design: The design of software and hardware will also be an enforcement focus, Szoka said.
• Mobile Devices: Companies should expect to see more data security cases related to mobile devices, Freeman said. Although usually the federal government lags behind industry developments, this government is not lagging far behind, he said.
• Data Brokers: "Protecting consumers from the excesses of the data broker industry will be a top agenda issue for the commission," Jeffrey Chester, executive director of the Center for Digital Democracy, said. "We expect the agency will call for legislation and also propose the industry adopt better consumer practices on transparency, disclosure and control."

LESSONS LEARNED FROM THE RED FLAGS RULE?

Court, Congress Found FTC'S Reach Exceeded Grasp
The FTC's original identity theft prevention and mitigation Red Flags Rule was never enforced because of controversy surrounding its scope. In 2007, the commission sought to apply the Fair and Accurate Credit Transactions Act rule more broadly to "creditors" than the financial regulators who jointly issued the rule (6 PVLR 1707, 11/5/07). The FTC sought to include any providers of goods and services, including attorneys and health-care providers, that regularly grant their customers the right to defer payments.

The commission was forced to implement several rule enforcement extensions in the face of industry pressure. It also faced lawsuits from professional groups representing lawyers, doctors and accountants. The American Bar Association convinced a federal court that the FTC overstepped its jurisdictional bounds (8 PVLR 1552, 11/2/09).

Congress stepped in while the ABA case was pending before an appeals court and ordered the FTC to narrow its definition of creditors (10 PVLR 8, 1/3/11). The commission issued a revised Red Flags Rule in December 2012 (11 PVLR 1763, 12/10/12).