A court is expected to rule on motions to dismiss in Federal Trade Commission v. Wyndham Worldwide Corp. any day. Some arguments made in support of the motion indicate that the “voluntary” cybersecurity framework being developed under President Obama’s February 2013 executive order could shape how regulators and the courts evaluate future private conduct, explain Wiley Rein LLP’s Megan L. Brown and Caroline R. Van Wie.

**FTC v. Wyndham Argument Underscores Importance of Developing Federal Cybersecurity Policy**

**By Megan L. Brown and Caroline R. Van Wie**

When the Federal Trade Commission picked a fight with Wyndham Hotels over data security following Russian cyber attacks, it ensured that its authority would be scrutinized. FTC v. Wyndham tests the FTC’s authority to punish companies for their data security practices following cybersecurity breaches. It also illustrates how federal cybersecurity policy, currently focused on critical infrastructure providers, could impact the private sector more broadly.

Depending on how it is drafted and used, a “voluntary” Cybersecurity Framework being developed under President Obama’s February 2013 executive order could be looked to as a guide to what is “reasonable” cybersecurity in the eyes of the FTC and courts.

The Legal Battle: A Snapshot

Between 2008 and 2010, cyber criminals hacked into the computer networks of Wyndham Hotels & Resorts and Wyndham-branded hotel franchises three times, resulting in the theft of customers’ payment card data from independent Wyndham franchises. After an investigation, the FTC sued, alleging that various Wyndham entities violated Section 5(a) of the Federal Trade Commission Act, which prohibits “unfair or deceptive acts or practices.” The FTC alleged that Wyndham, through its web site, disseminated privacy policies with which it did not comply, and a data breach occurred, constituting a “deceptive” business practice. The FTC also claimed that Wyndham failed to use “reasonable and appropriate” safeguards to protect the personal information collected and maintained by Wyndham’s corporate and franchisee systems, an alleged “unfair” business practice.

In the absence of clear guidance about what is reasonable data security, and with Congress struggling to reach consensus, companies should pay attention to the Cybersecurity Framework under development at National Institute of Standards and Technology. Depending on how it is written and deployed, that Framework could influence how regulators and courts evaluate private conduct in the future.

In April 2013, the Wyndham defendants moved to dismiss both counts. While the parties also dispute the “deception” allegation, the headline fight centers on the “unfair” practices claim. Wyndham challenges the FTC’s authority to punish firms for inadequate data se-
curity practices. It asserts that the agency lacks binding rules or guidance, and that the FTC cannot bring an enforcement action because it has never provided adequate notice of what qualifies as "reasonable" data security practices. Wyndham further argues that the FTC’s authority must be read narrowly because Congress did not intend to grant it general authority to police data security, and because FTC enforcement would usurp Congress’s policymaking role while debate over cybersecurity legislation is ongoing.

In response, the FTC argues that it has broad authority to regulate "unanticipated practices," and may seek remedies for data security breaches under Section 5(a). The FTC contends that it provided ample notice through prior enforcement actions, which brought about over a dozen consent decrees that illuminate what constitutes "reasonable" security. In response to the notion that congressional inertia confirms an absence of authority, the FTC notes that some proposed bills have included "savings clauses" that would preserve what it sees as existing agency powers.

The case has drawn the attention of diverse interests, including the U.S. Chamber of Commerce, the National Federation of Independent Business, TechFreedom, the International Franchise Association, and Public Citizen, which each filed amicus briefs. The court heard argument on the motions to dismiss on Nov. 7, and a decision is expected at any time. At the hearing, the court repeatedly asked whether Wyndham’s arguments are more appropriately addressed at summary judgment after discovery, signaling wariness about disposing of the case entirely on the pleadings.

'Voluntary' Standards Could Inform What Constitutes 'Reasonable' Data Security. At the hearing, the parties and the court spent quite some time on whether industry has enough regulatory guidance about what constitutes "reasonable" data security. There were repeated references to the Cybersecurity Framework currently being developed by National Institute of Standards and Technology (NIST). That Framework will be part of a "Voluntary Program" to be developed for owners and operators of critical infrastructure. But in the absence of regulatory guidance about appropriate cybersecurity, industry, courts, and regulators might look to the Framework for direction.

Counsel for Wyndham cited the still-developing Framework as a potential guide. Counsel noted that, in contrast to the status quo, if a company in the future "asked Homeland Security or [NIST] what hardware configurations are required for a proper network, I know now from President Obama's Executive Order, I know exactly what is required." Counsel continued: "if the FTC had done what the Department of Commerce and the Department of Homeland Security had done, and published certain guidelines, then this would be a far different argument." At other times, the Framework was characterized by Wyndham counsel as a potential safe harbor for private actors. While the Framework may not be intended for such use, this discussion illustrates the significance that may be attributed to it.

Whatever the conclusion in Wyndham, this is just one of many skirmishes over the adequacy of private-sector security to come. Those battles may not be limited to major critical infrastructure owners, but could involve companies of all sizes, many of which do not presently operate under the watchful eye of specialized regulators. In the absence of clear guidance about what is reasonable, and with Congress struggling to reach consensus, companies should pay attention to the Cybersecurity Framework under development at NIST. Depending on how it is written and deployed, that Framework could influence how regulators and courts evaluate private conduct in the future.

Megan L. Brown is a partner in Wiley Rein LLP’s Communications, Litigation, and Appellate practices. She represents corporations and industries in litigation and regulatory proceedings and develops compliance strategies under a variety of statutes.

Caroline R. Van Wie, an associate in Wiley’s Communications Practice, assists clients in a variety of regulatory, transactional, litigation, and compliance matters in the area of telecommunications.