LOS ANGELES
Daily Journal
www.dailyjournal.com
FRIDAY, APRIL 18, 2014

PERSPECTIVE

Case bolsters FTC's data security role

By Megan L. Brown and Scott D. Delacourt

Numerous parts of the federal government are gearing up to take action on cyber and data security, but little concrete has materialized. Congress has considered major legislation, but reached no consensus. Federal agencies are implementing the president's executive order on "Improving Cybersecurity for Critical Infrastructure," and are looking at what more they can do. In the meantime, the private sector lacks definitive or binding guidance about how to manage increasingly challenging cyber threats. In the absence of federal action, the Federal Trade Commission has taken an aggressive role, using its consumer protection authority to police private sector data security.

While the legal underpinning of this role has been challenged, a recent court victory for the FTC ensures that the agency will maintain its assertive role in data and cyber security. In *FTC v. Wyndham Worldwide Corp. et al.*, No. 13-1887 (D.N.J.), the FTC's jurisdiction to punish companies for allegedly lax data security practices was challenged when Wyndham moved to dismiss unfair and deceptive practices claims brought by the FTC after a breach. On April 7, U.S. District Judge Esther Salas rejected Wyndham' arguments and affirmed FTC jurisdiction. She noted that the case highlights "a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future."

The FTC is no stranger to data security. It administers several sector-specific statutes that impose data security obligations, including the Gramm-Leach-Bliley Act, which covers financial institutions; the Fair Credit Reporting Act, which regulates consumer reporting agencies, and the Children's Online Privacy Protection Act, which regulates commercial websites and online services directed to children. Other agencies have sector-specific data-security roles as well.

For years, the FTC has sought general regulatory authority over data security. On Feb. 4, in a prepared statement to the Committee on the Judiciary, the agency asserted general authority "to promote data security in the private sector through civil law enforcement, education, policy initiatives, and recommendations to Congress to enact legislation in this area."

As a legal matter, the FTC relies on the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act. See 15 U.S.C. Section 45(a). If a company makes materially misleading statements or omissions about data security, it can violate Section 5's bar on deceptive practices. The FTC has also begun to police data security under Section 5's "unfairness" provision. According to the FTC's statement, "if a company's data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5."

The FTC has published some guidance, but has not promulgated rules for general data security practices. Nonetheless, the FTC has brought and settled 50 cases against businesses for failing to provide reasonable protection for consumers' personal information. Resulting consent decrees often include monitoring periods of 20 years, so settling companies can expect lengthy compliance obligations. The FTC claims that its consent decrees provide the private sector with guidance about what is expected.

The agency's assertion of broad Section 5 authority over private sector data security has raised eyebrows. Companies facing legal expenses and reputational risk often do not want to tangle with the FTC and accede to consent decrees, but some have challenged the FTC's approach.

Wyndham Hotels

Wyndham Hotels & Resorts fought back. Between 2008 and 2010, Russian cyber criminals breached Wyndham Hotels & Resorts and Wyndham-branded franchise networks, stealing customer payment card data. After an investigation, the FTC sued, alleging that Wyndham violated Section 5(a) of the FTC Act, prohibiting "unfair or deceptive acts or practices." The FTC alleged Wyndham did not comply with its own disseminated privacy policies, and also that Wyndham failed to use "reasonable and appropriate" safeguards to protect personal information, which the FTC claimed was an "unfair" business practice.

In April 2013, Wyndham moved to dismiss both counts, attacking FTC authority over data security. The fight centered on the "unfair" practices claim, which Wyndham characterized as an impermissible expansion of FTC jurisdiction. Wyndham challenged the FTC's power to punish firms for their data security practices in the absence of clear rules or guidance about what constitutes "reasonable" data security. Wyndham argued that the FTC's jurisdiction is necessarily limited because Congress elsewhere provided specific data-security power, and because enforcement would usurp Congress's policy role. A coalition of business groups filed a brief supporting Wyndham, arguing that the FTC's "incremental — and unilateral — regulation-through-settlement subjects American businesses to vague, unknowable, and constantly changing data-security standards."

The parties also litigated the "deception" claim, disputing, among other things, whether the agency adequately pled consumer injury and whether the heightened pleading requirements under Federal Rule of Civil Procedure 9(b) apply to deception claims.

Salas rejected Wyndham's arguments about the FTC's jurisdiction, and denied the motion to dismiss.

The court affirmed the FTC's jurisdiction and its discretion to regulate through enforcement, rejecting Wyndham's argument that "the FTC's 'failure to publish any interpretive guidance whatsoever' violates fair notice principles and 'bedrock principles of administrative law.'" The court found Section 5's unfairness standard to be flexible and noted that the FTC had brought "unfairness actions in a variety of contexts without preexisting rules or regulations." Thus, the court found "inapposite" Wyndham's reference to evolving frameworks at the Department of Homeland Security and the National Institute of Standards and Technology as examples of what the FTC should do. The court analogized the FTC's approach to case-by-case adjudication used by the National Labor Relations Board and the Occupational Safety and Health Administration, rejecting Wyndham's argument that the "rapidly-evolving nature of data security" made those agencies poor examples.

The court also rejected the challenge to the deceptive practices claim, finding that the FTC had adequately pled it under whatever standard applied.

Future Uncertainty

The future of data and cybersecurity will be marked by uncertainty and litigation. The Wyndham court was clear that it was merely rejecting arguments to limit the FTC's authority and not passing on the hotels' security practices: "[a] liability determination is for another day." Unless they settle, the parties likely will proceed to costly discovery and further litigation over the adequacy of Wyndham's data security practices.

This green light enhances the FTC's power and promises that more companies will face scrutiny. Despite the court's statement that "this decision does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked," it provides a clear path to bring data security cases under the flexible "reasonableness standard" for unfair business practices.

As a result, legal battles will have to be fought over the adequacy of private-sector security. The court acknowledged that the future will be rocky, noting that "maintaining privacy is, perhaps, an ongoing struggle," and predicting that "Congress and the courts" will confront "thorny legal issues" for "the foreseeable future."

These thorny issues threaten to ensnare companies of all sizes, many of which do not now consider themselves heavily regulated. In the absence of clear guidance about what is reasonable, and with Congress struggling to reach consensus, companies must pay attention to what the FTC and other federal agencies are doing. The executive order on cybersecurity has kicked off a variety of regulatory actions. This includes the development and release of a Cybersecurity Framework in February by NIST, which federal agencies are looking to build on as part of an intended voluntary program for critical infrastructure owners and operators. The federal government is also exploring how to leverage its procurement power to improve private sector security practices by conditioning contracts on improved data security and supply chain management.

Unless an appeals court comes to a different conclusion or Congress takes action, companies should heed what the FTC and other agencies are doing on data and cybersecurity. This includes taking advantage of opportunities to comment on proposals percolating in the regulatory agencies. As policy develops, the private sector should expect more case-by-case enforcement actions to be brought by an empowered FTC, and burgeoning demands to crop up throughout federal regulation.

MEGAN L. BROWN
Wiley Rein LLP

Megan L. Brown *is a partner at Wiley Rein LLP. She can be reached at mbrown@wileyrein.com.*

SCOTT D. DELACOURT
Wiley Rein LLP

Scott D. Delacourt *is a partner at Wiley Rein LLP. He can be reached at sdelacourt@wileyrein.com.*