Foster Garvey

Duff on Hospitality Law

From Bad to Worse for Wyndham

on 8.27.15 | Posted in Data Privacy, FTC

Lawyers often say “bad facts make bad law”. Combine that with weak legal arguments and, well, things can get really bad, really fast. That’s precisely what happened to Wyndham yesterday when the Third Circuit affirmed a federal District Court decision that the Federal Trade Commission (“FTC”) has authority to regulate cybersecurity under the unfairness prong of § 45(a) of the Federal Trade Commission Act. While commentators may disagree on the result from a legal or policy perspective, one thing is for certain, it was a bad result for Wyndham. The decision rejected in no uncertain terms Wyndham's argument that the FTC lacked authority; and not kindly.

By now, the facts of the Wyndham debacle are well known. As summarized by the Third Circuit:

On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation's computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges.

The FTC ultimately filed suit in federal District Court alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive. Wyndham challenged the FTC's authority to regulate cybersecurity and sought to dismiss the action. The District Court denied Wyndham's motion to dismiss and Wyndham appealed.

On appeal, Wyndham presented essentially two arguments: (a) in addition to meeting the requirements of Section 45(n), its behavior must be “unscrupulous or unethical” to be actionable and (b) it did not have fair notice of the “specific cybersecurity standards” it was required to follow. The Third Circuit disposed of each of these arguments easily, leaving little doubt that if a company makes privacy or security claims for which it lacks reasonable basis, it will be held responsible.

As to the first argument, the Third Circuit both rejected the proposition and chided Wyndham for even raising it under the circumstances:

Next, citing one dictionary, Wyndham argues that a practice is only "unfair" if it is "not equitable" or is "marked by injustice, partiality, or deception." . . . Whether these are requirements of an unfairness claim makes little difference here. A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about

data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.

Furthermore, in response to Wyndham's argument that extending the FTC's reach to Wyndham's conduct would necessarily result in the FTC "regulat[ing] the locks on hotel rooms . . . [authorizing the FTC] to sue supermarkets that are "sloppy about sweeping up banana peels", the court said:

Th[is] argument is alarmist to say the least. And it invites the tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a).

Wyndham fared no better on its second argument. In disposing of it the court noted that Wyndham changed its position at least seven times throughout the appeal. The court resolved that: "Wyndham was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by § 45(a)", and that "Fair notice is satisfied as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute". The court elaborated, assuming that what Wyndham was really arguing was that the statute had not been fairly applied by the FTC because the FTC did not apply cost-benefit analysis required under §45(n), i.e. whether the harm to consumers was reasonably avoidable by consumers and not outweighed by countervailing benefits:

Wyndham's as-applied challenge falls well short given the allegation in the FTC complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all*, did not use *any* encryption for certain customer files, and did not require some users to change their default or factory-setting passwords *at all*. . . .

Wyndham's as-applied challenge is even weaker given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis.

In the end, the court stated:

Thus, Wyndham cannot argue that it was entitled to know with ascertainable certainty the cybersecurity standards by which the FTC expected it to conform. Instead, the company can only claim that it lacked fair notice of the meaning of the statue itself - a theory it did not meaningfully raise and that we strongly suspect would be unpersuasive under the facts of this case.

Bottom line, as far as this case goes, yesterday was not a good day for Wyndham. The appellate court's decision lays bare that Wyndham - once again – failed to learn from and even disregarded its prior experience to the detriment of its customers. Also, in response to Wyndham's direct challenge to the FTC's authority, the Third Circuit has now confirmed in an important published decision the FTC's authority to regulate cybersecurity under the unfairness prong of §45(a). Perhaps, if, faced with better facts (and arguments), the court may have reached a different result. But, certainly, when a company doesn't mind the "promise vs. performance" gap with respect to its public statements about security and its actual practices tempt fate, it risks the scrutiny of trade practice regulators and disappointed customers and their lawyers. The consequences of failure can be great: reputational harm, customer flight, lost sales, exposure of trade secrets, remedial efforts, litigation and associated costs and damages, and, as *Wyndham* illustrates, regulatory agency scrutiny and action.

To avoid this result, all companies that collect and store customer data need to measure carefully what they say and what they do against constantly evolving data security standards to confirm they are employing reasonable practices, and that their statements about privacy match their actions. This means examining FTC enforcement actions for guidance, industry and government standards/recommendations (see, e.g., *Framework for Improving Critical Infrastructure Cybersecurity*), and adjusting security practices accordingly. It also means dusting off and reviewing published and often-forgotten privacy policies to ensure they align with the steps actually taken to secure customer data, and, of course, actually taking reasonable steps to do so. Oh, and insurance; don't overlook cybersecurity insurance. The process of applying for it will likely expose flaws in security practices, and getting it will help offset the considerable costs of responding to a data breach incident. Remember, most experts agree that it is no longer a question of whether a data breach will occur, but when. Forewarned is forearmed.

***

Benjamin J. Lambiotte is a Principal at Foster Garvey, and is working out of its Washington, D.C. office.

Tags: customer data, cybersecurity, cybersecurity insurance, Data Breach, data privacy, data security standards, Federal Trade Commission, Federal Trade Commission Act, privacy and data security, Third Circuit, Wyndham, Wyndham Worldwide Corporations