Wyndham, Heartbleed, and the Pitfalls of Setting Cybersecurity Standards Through Litigation

by

Archis A. Parasharami & Stephen Lilley*

In the world of data breaches and cybersecurity, 2014 has already been an eventful year before it is even half over. In recent weeks, the Heartbleed bug has launched hundreds of headlines, if not more—following on the heels of reports of one high-profile breach after another.[1] In the wake of these reports, mitigation costs for companies victimized by network intrusions and data breaches are continuing to soar.[2] And (inevitably) litigation has sprung up at every turn, seeking to impose liability for alleged violations of data-security standards that, in our view, have been discovered post hoc and with little regard for the defendant's cybersecurity efforts.

All of these developments have taken place against the backdrop of a continuing debate about how the nation should respond to the potentially severe cybersecurity-related threats to its national and economic security as well as to sensitive personal and business information. On one point, however, there is a growing consensus: Nearly everyone agrees that our national strategy must include a public-private partnership for the development of broadly applicable cybersecurity standards. This view—reflected in the recently-announced National Institute for Standard and Technology's Cybersecurity Framework[3]—recognizes that the private and public sectors must work together to strengthen our nation's cybersecurity. It likewise recognizes that one-size-fits-all checklists are inferior to risk-based cybersecurity practices, and that real-time cooperation is vastly superior to rigid regulation that can rapidly (perhaps instantly) become obsolete. Thus, an ever-expanding group of stakeholders share the common goal of leveraging market forces—whether through insurance contracts, investor demands, or customer/vendor requirements—to ensure that all companies have appropriate cybersecurity practices and procedures aimed at mitigating the risks that they face.[4]

By contrast, the value of regulation-by-litigation in response to cyber incidents and threats is far less clear. Indeed, whether such matters belong in court at all has (appropriately) proven to be

* Archis A. Parasharami is a litigation partner in Mayer Brown's Washington, D.C. office and co-chair of the firm's Consumer Litigation and Class Action Practice. Stephen Lilley is an associate with the firm.

1 *See, e.g.*, Jim Finkle, *Little Internet Users Can Do to Thwart 'Heartbleed' Bug*, Reuters (Apr. 9, 2014).

2 *See, e.g.*, 2014 Verizon Data Breach Investigations Report (2014), *available at* http://www.verizonenterprise.com/DBIR/2014/.

3 *See* Press Release, National Institute of Standards and Technology, NIST Releases Cybersecurity Framework Version 1.0 (Feb. 12, 2014), *available at* http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

4 *See generally* Background Briefing on the Launch of the Cybersecurity Framework (Feb. 12, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/02/12/background-briefing-launch-cybersecurity-framework.

a significant threshold question. Countless putative class actions have been brought by plaintiffs asserting claims about data breaches, large and small. These lawsuits are not filed against the unknown hackers, of course, but instead against the companies that themselves were victimized. But courts often reject these lawsuits for lack of standing, because plaintiffs frequently fail to allege or demonstrate that they have suffered any particularized injury (as opposed to a general heightened fear of identity theft).[5]

Nonetheless, not every such case is dismissed for lack of standing, and recent developments suggest that these lawsuits may become even more common. One potential trigger: In the closely-watched *Wyndham* case, a federal district court recently held that the Federal Trade Commission (FTC) may use its broad and vague "unfairness" authority under Section 5(a) of the FTC Act to enforce data-security standards. This move is likely to encourage further FTC enforcement actions and follow-on private litigation. But whether such litigation will be common and whether it will be a good idea—more specifically, whether setting de facto standards through FTC enforcement actions or private class actions is wise cybersecurity policy—are two different questions.

In our view, the use of litigation in response to data breaches and other cyber incidents is highly unlikely to identify and drive the adoption of constructive cybersecurity standards. To the contrary, setting such standards through after-the-fact litigation conflicts with the collaborative approach that created the Cybersecurity Framework and the adoption of risk-based cybersecurity practices that it is intended to encourage. The problem with a litigation-focused approach to data security is that it is more likely to promote static security checklists and a one-size-fits-all approach to data security, when—as recent events on the ground suggest—what is really called for is a nimble and flexible approach to fighting cybersecurity threats. By seeking to impose liability through second guessing with the benefit of hindsight, cybersecurity litigation can be expected to dampen, rather than encourage, risk-based decision making by businesses.

The *Wyndham* Case

The *Wyndham* action arose when a group of hackers allegedly penetrated the hospitality chain's networks from 2008 to 2010, thereby compromising over a half-million payment card numbers. Wyndham, which already faced a substantial prospect of financial and reputational harm caused by the hackers' crime, next found itself facing a civil action filed by the FTC. In that lawsuit, the FTC alleged that Wyndham had not maintained reasonable and appropriate data-security measures.[6] The agency claimed that Wyndham had engaged in (1) deception through alleged misrepresentations

[5] *See, e.g., In re. Barnes & Noble Pin Pad Litigation*, No. 12–cv–8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013).

[6] *See* Complaint, *FTC v. Wyndham Worldwide Corp.*, Case No. 13-cv-01887 (D.N.J. June 26, 2012); Amended Complaint, *FTC v. Wyndham Worldwide Corp.*, Case No. 13-cv-01887 (D.N.J. Aug. 9, 2012).

of the company's data-security practices; and (2) "unfair" conduct based upon the harms allegedly suffered as a result of the purportedly unreasonable data-security practices.

Wyndham moved to dismiss the amended complaint, arguing, among other things, that the FTC's "unfairness" authority does not extend to data security, that the FTC had failed to provide fair notice of what Section 5 of the FTC Act requires, and that Section 5 does not govern the security of payment card data.[7] Wyndham—joined by a number of *amici*[8]—pointed to the FTC's lack of clear statutory authority, the continued legislative debates about data-security standards, and the FTC's failure to establish standards through rulemaking as powerful reasons why the FTC lacked the authority to regulate data-security practices through Section 5 enforcement actions.

The district court was not persuaded. It concluded that more narrow data-security requirements enacted by Congress complemented, rather than precluded, the FTC's assertion of authority under Section 5.[9] The court also disagreed with defendants about the import of the ongoing legislative debates and prior statements by the FTC about the limits of its authority to regulate data security.[10] The court thus declined "to carve out" what it understood to be "a data-security exception to the FTC's authority."[11] The court likewise held that the FTC did not need to promulgate rules before exercising that authority, and that the FTC had adequately pled its unfairness claim.[12] Finally, the court rejected the defendants' challenge to the FTC's deception claim.[13]

As a result of the *Wyndham* decision, companies can expect the FTC to continue—and perhaps even expand—its efforts to regulate data-security standards through enforcement actions. Indeed, many observers believe that the district court's decision—and the resulting headlines[14]—may serve to boost the FTC's efforts to regulate data security. This change will have at least three significant negative effects.

First, past FTC actions have spawned follow-on class litigation. Continued or possibly expanded FTC activity in the field of data security thus does not bode well for companies that must defend themselves first from hackers and then from regulators and plaintiffs' attorneys who seek

[7] Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC, *FTC v. Wyndham Worldwide Corp.*, Case No. 13-cv-01887 (D.N.J. April 26, 2013).

[8] *See, e.g.*, Brief of Amicus Curiae U.S. Chamber of Commerce, *FTC v. Wyndham Worldwide Corp.*, Case No. 13-cv-01887 (D.N.J. Oct. 5, 2012).

[9] *See FTC v. Wyndham Worldwide Corp.*, --- F. Supp. 2d ---, Case No. 13-cv-0188, 2014 WL 1349019 *7 (D.N.J. Apr. 7, 2014).

[10] *Id.* at *5-9.

[11] *Id.* at *4.

[12] *Id.* at *15-16.

[13] *Id.* at *25.

[14] *See, e.g.*, Brent Kendall, *Judge Backs FTC's Authority in Data-Breach Case*, WallStreetJournal.com (Apr. 7, 2014).

to turn a company's victimization into a basis for claimed liability. Likewise it ensures that further resources will be diverted away from cyberthreat risk-management and instead directed towards managing against the risk of litigation.

Second, the district court's highlighting of what it called "data-security insufficiencies" foreshadows a focus on simplistic checklists rather than on risk-based data-security practices.[15] These supposed "insufficiencies" include allegations that the company stored unencrypted data, used outdated operating systems, and failed to require the use of complex passwords. These purported "insufficiencies" were described in a manner bereft of any context—and in particular, without any reference to the specific risks facing the company or the company's overall security response. Yet data security is not one-size-fits-all. Context does matter: every network and associated risk profile is different, and a company's cybersecurity posture cannot be simplified down to a handful of technological decisions.[16] For that reason, the creation of a data-security checklist through litigation, whether by the FTC or by a putative class representative, will benefit no one.

Third, the district court's willingness to authorize case-by-case development of data-security standards—including through the use of consent orders that provide little or no guidance to non-parties—promises legal and regulatory uncertainty for companies in an area that cries out for stable and predictable guidelines. This uncertainty will only increase if class actions are allowed to further complicate the existing patchwork of data-security standards.

At bottom, the *Wyndham* decision is troubling for companies that seek to manage data-security risks and stave off unnecessary and inappropriate litigation. Indeed, the district court appeared resigned to the prospect of more litigation in this area, noting that "we live in a digital age that is rapidly evolving" and that will raise "a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future." Companies certainly should hope that the district court was wrong to forecast more litigation, but should be prepared for continued legal uncertainty and the opportunistic litigation it will generate. We should not have high hopes that improved data security will follow.

The Heartbleed Bug

If the decision in *Wyndham* is a bombshell in the world of cybersecurity law, the recent (and widespread) news of the Heartbleed bug set off fireworks of its own in the technological arena. The origins and operation of the Heartbleed bug have been well catalogued.[17] In short, it is a vulner-

[15] *See id*. at *19.

[16] *See* NIST, Cybersecurity Framework v. 1.0, at 2 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf ("The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary.").

[17] *See generally* Brian Krebs, Krebs on Security, *'Heartbleed' Bug Exposes Passwords, Web Site Encryp-*

ability in the widely-used open source Secure Sockets Layer (SSL) encryption protocol that can allow a hacker to access the information stored on a device using that technology. This vulnerability is significant since that information may include encryption keys, passwords, or other sensitive information.

A few basic points about the Heartbleed bug merit emphasis. First, the vulnerability is a simple one, as are the techniques for exploiting that vulnerability. Second, to the extent that the Heartbleed vulnerability was not exploited by hackers, it was because the vulnerability remained undiscovered, unlike other "zero day vulnerabilities" that are traded on a thriving black market. Third, because of the broad use of the SSL technology, the Heartbleed vulnerability found its way into an enormous number of websites, as well as pieces of hardware, resulting in significant remediation challenges and expense. Thus, the Heartbleed bug was one that companies likely could and would have protected their networks against—*if* they had they known about the vulnerability—but that now imposes significant remediation challenges because of how long the vulnerability was unrecognized.

But should litigation play any role in addressing such a vulnerability? In our view, the answer is no: the Heartbleed bug, arriving on the heels of the *Wyndham* decision, provides a compelling example of why FTC enforcement actions and private litigation are unlikely to improve cybersecurity standards.

As noted above, though the Heartbleed bug was simple, "reasonable security procedures" could not be expected to identify any exploitation of this vulnerability, or even the vulnerability itself. In our view, a company's data-security practices cannot be deemed unreasonable—and the FTC thus cannot state an unfairness claim—simply because of such an unknown vulnerability that was shared by large numbers of sophisticated online merchants as well as providers of email and countless other popular services. Conversely, "reasonable security procedures" cannot be expected to prevent the most sophisticated hackers, using the most advanced tools, from penetrating a company's networks. Thus, the FTC's "unfairness" authority should apply only to a limited set of instances, from which unknown threats and highly sophisticated threats ought to be excluded.

These limitations call into question the out-sized role that the FTC has claimed with respect to data-security law and policy. The FTC should be very careful not to exercise this asserted authority in a way that causes companies to prioritize cybersecurity resources towards fending off litigation risks and away from the broad swath of cyber risks to which the FTC does not speak. Companies should be working collaboratively and in real-time with the federal government and each other to respond in a risk-based manner (not a litigation-avoidance-based manner) to the full set of threats

---

tion Keys (Apr. 8, 2014), *available at* http://krebsonsecurity.com/2014/04/heartbleed-bug-exposes-passwords-web-site-encryption-keys/; Graham Clulely, *Heartbleed Bug Explained by xkcd in a Way Anyone Can Understand* (Apr. 11, 2014), *available at* http://grahamcluley.com/2014/04/heartbleed-bug-explained/.

facing their networks. They should not constantly have to look over their shoulders or read the tea leaves of past FTC actions for fear of being second guessed by the FTC.

The Heartbleed bug likewise demonstrates the limitations of class-action litigation in the data breach context. Given the widespread use and industry acceptance of the open source SSL protocol, private plaintiffs would likely fail to state a claim for negligence or failure to meet standards of commercial reasonableness (or any other standard other than strict liability, for that matter). It is not reasonable to expect that any company should have made itself immune to the Heartbleed bug before it was discovered and publicized. For the most part, then, it seems unlikely that class actions launched over the Heartbleed bug will gain much traction, although perhaps some plaintiffs' lawyers will try.

In our view, such efforts would be unfortunate. Risk-based cybersecurity practices, in which defined resources are allocated against perceived threats according to the anticipated level of risk, inevitably require hard decisions and judgment calls. Allowing the plaintiffs' bar to string together a few of these hard decisions into a narrative drawn with the benefit of hindsight is neither fair nor productive. Companies should be encouraged to explore their risks and make business judgments in response—these discussions and judgments should not be chilled by the threat of second guessing through litigation.

~~~~~

If courts permit the use of enforcement actions and class action litigation to generate data-security standards on a post hoc basis, that approach would run the risk of imposing potentially massive liability on companies. At the same time, it would threaten to turn companies' focus away from appropriate cybersecurity practices based on risk and instead towards wooden compliance with a checklist of practices that may reduce future liability risk, but do not advance enterprise security. As the *Wyndham* case and the Heartbleed bug illustrate, the blunt instruments of FTC enforcement actions and class action litigation are likely to generate only waste and confusion in the arena of cybersecurity. Courts, policymakers, and the public should demand better.
~~~~~