UNDER CISA, WOULD WYNDHAM BE ABLE TO PRE-EMPT FTC ACTION?

The Third Circuit just issued an important ruling holding that the Federal Trade Commission could sue Wyndham Hotels for having cybersecurity practices that did not deliver what their privacy policies promised. The opinion, written by Clinton appointee Thomas Ambro, laid out just how bad Wyndham's cybersecurity was, even after it had been hacked twice. Ambro upheld the District Court's decision that FTC could claim that Wyndham had unfairly exposed its customers.

> The Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a). In 2005 the Federal Trade Commission began bringing administrative actions under this provision against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. The vast majority of these cases have ended in settlement.
>
> 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 filed suit in federal District Court, alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham's motion to dismiss, and we granted interlocutory appeal on two issues: whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair

> notice its specific cybersecurity practices could fall short of that provision.1 We affirm the District Court.
>
> [snip]
>
> Wyndham's as-applied challenge falls well short given the allegations in the FTC's 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, Compl. at ¶ 24(a), did not restrict specific IP addresses at all, id. at ¶ 24(j), did not use any encryption for certain customer files, id. at ¶ 24(b), and did not require some users to change their default or factory-setting passwords at all, id. at ¶ 24(f). Wyndham did not respond to this argument in its reply brief.
>
> 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 costbenefit analysis. That said, we leave for another day whether Wyndham's alleged cybersecurity practices do in fact fail, an issue the parties did not brief. We merely note that certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court could find that its practices fail the cost-benefit analysis.

The ruling holds out the possibility that threats of such actions by the FTC, which has been hiring superb security people in the last several years, might get corporations to adopt

better cybersecurity and thereby make us all safer.

Which brings me to an issue I've been asking lots of lawyers about, without satisfactory answer, on other contexts.

The Cybersecurity Information Sharing Act prevents the federal government, as a whole, from bringing any enforcement actions against companies using cybersecurity threat indicators and defensive measures (or lack thereof!) turned over voluntarily under the act.

> (D) FEDERAL REGULATORY AUTHORITY.—
>
> (i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this Act shall not be directly used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any entity, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.
>
> (ii) EXCEPTIONS.—
>
> (I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators and defensive measures provided to the Federal Government under this Act may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.
>
> (II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS ACT.—Clause (i) shall not apply to procedures developed and implemented under this Act.

Given this precedent, could Wyndham — and other negligent companies — pre-empt any such FTC actions simply by sharing promiscuously as soon as they discovered the hack?

Could FTC still sue Wyndham because it broke the law because it claimed its "operating defensive measures" were more than what they really were? Or would such suits be precluded — by all federal agencies — under CISA, assuming companies shared the cyberattack data? Or would CISA close off this new promising area to force companies to provide minimal cybersecurity?

Update: Paul Rosenzweig's post on the FTC decision is worth reading. Like him, I agree that FTC doesn't yet have the resources to be the police on this matter, though I do think they have the smarts on security, unlike most other agencies.