LabMD Update

by John Conley

Last September, I reported on the Federal Trade Commission's decision upholding its enforcement action against the now-defunct clinical laboratory LabMD, Inc. In 2013, the FTC brought an administrative complaint against LabMD, alleging that its lax cybersecurity practices resulted in the exposure of patient data. As I wrote last year, *exposure* was the key word, as the FTC did not allege any actual data theft or other tangible harm to patients.

When LabMD challenged the FTC's authority to bring such a complaint, an Administrative Law Judge (theoretically independent, though an FTC employee) agreed in a 2015 decision—apparently the first time that a company has successfully challenged an FTC complaint alleging unreasonable security practices. The FTC appealed to the Federal Trade Commission (to itself, in effect), and the FTC Commissioners reversed the ALJ and issued a final order compelling LabMD to implement new and better security measures. LabMD then appealed the FTC's order to the U.S. Court of Appeals for the Eleventh Circuit, which sits in Atlanta and hears cases from Alabama, Florida, and Georgia. A three-judge panel of that court heard oral argument from the parties' lawyers on June 21, 2017, and its decision is pending.

In my earlier post, I noted several distinctive aspects of the case. The first is that it signaled the FTC's move into the health privacy area. Clinical labs like LabMD are usually not covered by HIPAA, since they are neither health care providers nor "business associates" of the latter, nor are they subject to any other sector-specific federal privacy laws. The *LabMD* case reflects the FTC's intent to fill that gap and regulate otherwise unregulated health-related businesses.

A second point concerned the FTC's right to regulate data security at all. As I wrote, the FTC originally just required companies to live up to whatever privacy *policies* they announced. The more recent trend, reflected in *LabMD*, is to evaluate the substantive adequacy of privacy and data security *practices*. The FTC claims this right under section 5(a) of the FTC Act, which authorizes the FTC to prohibit and police "unfair or deceptive acts or practices in or affecting commerce." As I described it in the earlier post, the FTC's "regulatory algorithm is that unreasonable privacy practices=unfair trade practices, and thus violate section 5." The FTC's authority to do this has been upheld by multiple courts, including another U.S. Court of Appeals—the Third Circuit in Philadelphia—in the 2015 *Wyndham Hotels* case. The *Wyndham* decision is not binding on the Eleventh Circuit in this case, but there is no indication that the court will revisit that issue here.

A third and related point concerns the FTC's specific authority to take enforcement action under the precise circumstances of this case. As I noted above, there is no allegation of actual harm to patients, just the possibility of harm. The FTC relies on section 5(n) of the FTC Act, which authorizes it to take enforcement action if "the act or practice causes or is likely to cause substantial injury to consumers." As reflected in the oral argument, the key question in this case is whether the mere exposure of the patients' data is sufficiently "likely to cause substantial injury."

(The argument can be heard on the court's website.)

I always caution people not to read too much into judges' questions during oral arguments. Aggressively probing the parties' positions is part of the job. This case might be the exception that proves the rule, however. I have rarely heard an argument that seemed so one-sided.

LabMD's lawyer faced some initial skepticism over whether the case is *moot*—no longer a live dispute that requires a decision—since the company ceased its testing business in 2014. He responded that LabMD is still an active corporation with an ongoing duty to keep patient records. He faced relatively little resistance in making his two main arguments on the meaning of section 5(n): that the mere possibility of unauthorized access, without tangible harm, doesn't amount to *substantial injury*; and that a "low-likelihood" harm isn't sufficiently *likely*.

(An aside: In cases brought by private parties alleging data exposure, courts have split on the question of how immediate or tangible the harm to the plaintiffs must be. The general trend, however, is that the mere potential of tangible harm is not enough. Just within the past few days, for example, a federal judge in California has dismissed a class action against Facebook for tracking its logged-out users' Internet activity, in part because of the absence of sufficiently "particularized and concrete" harm.)

In trying to rebut these arguments, the FTC's lawyer was absolutely hammered. I can only characterize the judges' tone as sarcastic; substantively, it seemed as if they were lying in wait to shred the FTC's contentions. For example, when the lawyer attempted an ill-advised analogy to private tort suits, the judges' withering—and well-prepared—criticisms forced him to back down and concede the point.

Perhaps most significant was the judges' recurrent concern about the FTC's effort to make general policy through individual enforcement cases. Characterizing this approach as "about as nebulous as you can get," the judges asked why the FTC didn't follow the formal rulemaking procedure specified by the Administrative Procedure Act, which provides the overarching framework for all federal regulatory action. Their specific concern seemed to be that the case-by-case approach puts no limits on the FTC's authority and offers affected businesses insufficient notice of what the FTC may view as illegal.

I wrote last June on the topic of informal agency policy-setting ("governance-by-guidance," as I called it) in the context of Myriad's dispute with the U.S. Department of Health and Human Services over patients' rights to their raw genomic sequencing data. The practical motivation for the FTC here, and HHS there, is that formal rulemaking is a long and complicated process, and can pin the agency down to a position that it may regret in the future. But, as I wrote a year ago, governance-by-guidance "can come out of the blue, with no advance notice or opportunity for public comment." As a consequence, it may promote "the assertion of power that agencies may not actually have." The judges' questions in the *LabMD* argument seemed to embody the very same concerns.

I emphasize yet again that it is dangerous to predict the outcome of a case from the tenor of judges' questions. But I'll ignore my own advice

and speculate that the FTC may have overreached in *LabMD*. I'll be very surprised if the decision doesn't result in at least some limits on the FTC's enforcement authority in the health privacy area.