ICLE International Center for Law & Economics

For LabMD, the Devil is in the Not-So-Well Specified Details
June 14, 2018
Geoffrey A. Manne, Gus Hurwitz and Kristian Stout

The Eleventh Circuit's *LabMD* opinion came out last week and has been something of a rorschach test for those of us who study consumer protection law.

Neil Chilson found the result to be a disturbing sign of slippage in Congress's command that the FTC refrain from basing enforcement on "public policy." Berin Szóka, on the other hand, saw the ruling as a long-awaited rebuke against the FTC's expansive notion of its "unfairness" authority. Whereas Daniel Solove and Woodrow Hartzog described the decision as "quite narrow and… far from crippling," in part, because "[t]he opinion says very little about the FTC's general power to enforce Section 5 unfairness." Even among the ICLE crew, our understandings of the opinion reflect our priors, from it being best understood as expressing due process concerns about injury-based enforcement of Section 5, on the one hand, to being about the meaning of Section 5(n)'s causation requirement, on the other.

You can expect to hear lots more about these and other *LabMD*-related issues from us soon, but for now we want to write about the only thing more exciting than dueling histories of the FTC's 1980 Unfairness Statement: administrative law.

While most of those watching the *LabMD* case come from some nexus of FTC watchers, data security specialists, and privacy lawyers, the reality is that the case itself is mostly about administrative law (the law that governs how federal agencies are given and use their power). And the court's opinion is best understood from a primarily administrative law perspective.

From that perspective, the case should lead to some significant introspection at the Commission. While the FTC may find ways to comply with the letter of the opinion without substantially altering its approach to data security cases, it will likely face difficulty defending that approach before the courts. True compliance with this decision will require the FTC to define what makes certain data security practices unfair in a more-coherent and far-more-readily ascertainable fashion.

# The devil is in the (well-specified) details

The actual holding in the case comes in Part III of the 11th Circuit's opinion, where the court finds for LabMD on the ground that, owing to a fatal lack of specificity in the FTC's proposed order, "the Commission's cease and desist order is itself unenforceable." This is

the punchline of the opinion, to which we will return. But it is worth spending some time on the path that the court takes to get there.

It should be stressed at the outset that Part II of the opinion — in which the Court walks through the conceptual and statutory framework that supports an "unfairness" claim — is surprisingly unimportant to the court's ultimate holding. This was the meat of the case for FTC watchers and privacy and data security lawyers, and it is a fascinating exposition. Doubtless it will be the focus of most analysis of the opinion.

But, for purposes of the court's disposition of the case, it's of (perhaps-frustratingly) scant importance. In short, the court assumes, *arguendo*, that the FTC has sufficient basis to make out an unfairness claim against LabMD before moving on to Part III of the opinion analyzing the FTC's order given that assumption.

It's not clear why the court took this approach — and it is dangerous to assume any particular explanation (although it is and will continue to be the subject of much debate). There are several reasonable explanations for the approach, ranging from the court thinking it obvious that the FTC's unfairness analysis was correct, to it side-stepping the thorny question of how to define injury under Section 5, to the court avoiding writing a decision that could call into question the fundamental constitutionality of a significant portion of the FTC's legal portfolio. Regardless — and regardless of its relative lack of importance to the ultimate holding — the analysis offered in Part II bears, and will receive, significant attention.

The FTC has two basic forms of consumer protection authority: It can take action against 1) *unfair* acts or practices and 2) *deceptive* acts or practices. The FTC's case against LabMD was framed in terms of unfairness. Unsurprisingly, "unfairness" is a broad, ambiguous concept — one that can easily grow into an amorphous blob of ill-defined enforcement authority.

As discussed by the court (as well as by us, *ad nauseum*), in the 1970s the FTC made very aggressive use of its unfairness authority to regulate the advertising industry, effectively usurping Congress' authority to legislate in that area. This over-aggressive enforcement didn't sit well with Congress, of course, and led it to shut down the FTC for a period of time until the agency adopted a more constrained understanding of the meaning of its unfairness authority. This understanding was communicated to Congress in the FTC's 1980 Unfairness Statement. That statement was subsequently codified by Congress, in slightly modified form, as Section 5(n) of the FTC Act.

Section 5(n) states that

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves

> and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

The meaning of Section 5(n) has been the subject of intense debate for years (for example, here, here and here). In particular, it is unclear whether Section 5(n) defines a test for what constitutes unfair conduct (that which "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition") or whether instead imposes a necessary, but not necessarily sufficient, condition on the extent of the FTC's authority to bring cases. The meaning of "cause" under 5(n) is also unclear because, unlike causation in traditional legal contexts, Section 5(n) also targets conduct that is "likely to cause" harm.

Section 5(n) concludes with an important, but also somewhat inscrutable, discussion of the role of "public policy" in the Commission's unfairness enforcement, indicating that that Commission is free to consider "established public policies" as evidence of unfair conduct, but may not use such considerations "as a primary basis" for its unfairness enforcement.

## Just say no to public policy

Section 5 empowers and directs the FTC to police unfair business practices, and there is little reason to think that bad data security practices cannot sometimes fall under its purview. But the FTC's efforts with respect to data security (and, for that matter, privacy) over the past nearly two decades have focused *extensively* on developing what it considers to be a comprehensive jurisprudence to address data security concerns. This creates a distinct impression that the FTC has been using its unfairness authority to develop a new area of public policy — to legislate data security standards, in other words — as opposed to policing data security practices that are unfair under established principles of unfairness.

This is a subtle distinction — and there is frankly little guidance for understanding when the agency is acting on the basis of public policy versus when it is proscribing conduct that falls within the meaning of unfairness.

But it is an *important* distinction. If it is the case — or, more precisely, if the courts think that it is the case — that the FTC is acting on the basis of public policy, then the FTC's data security efforts are clearly problematic under Section 5(n)'s prohibition on the use of public policy as the primary basis for unfairness actions.

And this is where the Commission gets itself into trouble. The Commission's efforts to develop its data security enforcement program looks an awful lot like something being driven by public policy, and not so much as merely enforcing existing policy as captured by,

in the *LabMD* court's words (echoing the FTC's pre-Section 5(n) unfairness factors), "well-established legal standard[s], whether grounded in statute, the common law, or the Constitution."

The distinction between effecting public policy and enforcing legal norms is… not very clear. Nonetheless, exploring and respecting that distinction is an important task for courts and agencies.

Unfortunately, this case does not well describe how to make that distinction. The opinion is more than a bit muddled and difficult to clearly interpret. Nonetheless, reading the court's dicta in Part II is instructive. It's clearly the case that some bad security practices, in some contexts, can be unfair practices. So the proper task for the FTC is to discover how to police "unfairness" within data security cases rather than setting out to become a first-order data security enforcement agency.

## How does public policy become well-established law?

Part II of the Eleventh Circuit's opinion — even if dicta — is important for future interpretations of Section 5 cases. The court goes to great lengths to demonstrate, based on the FTC's enforcement history and related Congressional rebukes, that the Commission may not rely upon vague "public policy" standards for bringing "unfairness" actions.

But this raises a critical question about the nature of the FTC's unfairness authority. The Commission was created largely to police conduct that could not readily be proscribed by statute or simple rules. In some cases this means conduct that is hard to label or describe in text with any degree of precision — "I know it when I see it" kinds of acts and practices. In other cases, it may refer to novel or otherwise unpredictable conduct that could not be foreseen by legislators or regulators. In either case, the very purpose of the FTC is to be able to protect consumers from conduct that is not necessarily proscribed elsewhere.

This means that the Commission must have some ability to take action against "unfair" conduct that has not previously been enshrined as "unfair" in "well-established legal standard[s], whether grounded in statute, the common law, or the Constitution." But that ability is not unbounded, of course.

The court explained that the Commission could expound upon what acts fall within the meaning of "unfair" in one of two ways: It could use its rulemaking authority to issue Congressionally reviewable rules, or it could proceed on a case-by-case basis.

In either case, the court's discussion of how the Commission is to determine what is "unfair" within the constraints of Section 5(n) is frustratingly vague. The earlier parts of the opinion tell us that unfairness is to be adjudged based upon "well-established legal standards," but here the court tells us that the scope of unfairness can be altered — that is, those well-established legal standards can be changed — through adjudication. It is difficult to square what the court means by this. Regardless, it is the guidance that we have been given by the

court.

## This is Admin Law 101

And yet perhaps there is some resolution to this conundrum in administrative law. For administrative law scholars, the 11th Circuit's discussion of the permissibility of agencies developing binding legal norms using either rulemaking or adjudication procedures, is straight out of *Chenery II*.

*Chenery II* is a bedrock case of American administrative law, standing broadly for the proposition (as echoed by the 11th Circuit) that agencies can generally develop legal rules through either rulemaking or adjudication, that there may be good reasons to use either in any given case, and that (assuming Congress has empowered the agency to use both) it is primarily up to the agency to determine which approach is preferable in any given case.

But, while *Chenery II* certainly allows agencies to proceed on a case-by-case basis, that permission is not a broad license to eschew the development of determinate legal standards. And the reason is fairly obvious: if an agency develops rules that are difficult to know *ex ante*, they can hardly provide guidance for private parties as they order their affairs.

*Chenery II* places an important caveat on the use of case-by-case adjudication. Much like the judges in the *LabMD* opinion, the *Chenery II* court was concerned with specificity and clarity, and tells us that agencies may not rely on vague bases for their rules or enforcement actions and expect courts to "chisel" out the details. Rather:

> If the administrative action is to be tested by the basis upon which it purports to rest, **that basis must be set forth with such clarity as to be understandable. It will not do for a court to be compelled to guess at the theory underlying the agency's action**; nor can a court be expected to chisel that which must be precise from what the agency has left vague and indecisive. In other words, 'We must know what a decision means before the duty becomes ours to say whether it is right or wrong.' (emphasis added)

The parallels between the 11th Circuit's opinion in *LabMD* and the Supreme Court's opinion in *Chenery II* 70 years earlier are uncanny. It is also not very surprising that the 11th Circuit opinion would reflect the principles discussed in *Chenery II*, nor that it would do so without reference to *Chenery II*: these are, after all, bedrock principles of administrative law.

The principles set out in *Chenery II*, of course, do not answer the data-security law question whether the FTC properly exercised its authority in this (or any) case under Section 5. But they do provide an intelligible basis for the court sidestepping this question, and asking whether the FTC sufficiently *defined* what it was doing in the first place.

# Conclusion

The FTC's data security mission has been, in essence, a voyage of public policy exploration. Its method of case-by-case adjudication, based on ill-defined consent decrees, non-binding guidance documents, and broadly-worded complaints creates the vagueness that the Court in *Chenery II* rejected, and that the 11th Circuit held results in unenforceable remedies.

Even in its best light, the Commission's public materials are woefully deficient as sources of useful (and legally-binding) guidance. In its complaints the FTC does typically mention some of the facts that led it to investigate, and presents some rudimentary details of how those facts relate to its Section 5 authority. Yet the FTC issues complaints based merely on its "reason to believe" that an unfair act has taken place. This is a far different standard than that faced in district court, and undoubtedly leads the Commission to construe facts liberally in its own favor.

Moreover, targets of complaints settle for myriad reasons, and no outside authority need review the sufficiency of a complaint as part of a settlement. And the consent orders themselves are largely devoid of legal and even factual specificity. As a result, the FTC's authority to initiate an enforcement action  is effectively based on an ill-defined series of hunches — hardly a sufficient basis for defining a clear legal standard.

So, while the court's opinion in this case was narrowly focused on the FTC's proposed order, the underlying legal analysis that supports its holding should be troubling to the Commission.

The specificity the 11th Circuit demands in the remedial order must exist no less in the theories of harm the Commission alleges against targets. And those theories cannot be based on mere public policy preferences. Courts that follow the Eleventh Circuit's approach — which indeed Section 5(n) reasonably seems to require — will look more deeply into the Commission's allegations of "unreasonable" data security in order to determine if it is actually attempting to pursue harms by proving something like negligence, or is instead simply ascribing "unfairness" to certain conduct that the Commission deems harmful.

The FTC may find ways to comply with the letter of this particular opinion without substantially altering its overall approach — but that seems unlikely. True compliance with this decision will require the FTC to respect real limits on its authority and to develop ascertainable data security requirements out of much more than mere consent decrees and kitchen-sink complaints.

View Article