ORAL ARGUMENT HELD JANUARY 9, 2018
PANEL DECISION ISSUED JUNE 1, 2018

NO. 17-5128

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

MICHAEL J. DAUGHERTY AND LABMD, INC.,

Petitioners,

v.

ALAIN H. SHEER, in his individual capacity
and RUTH T. YODAIKEN, in her individual capacity,

Respondents.

On Appeal from the United States District Court
for the District of Columbia

PETITION OF MICHAEL J. DAUGHERTY AND LABMD, INC. FOR PANEL REHEARING OR, IN THE ALTERNATIVE, FOR REHEARING *EN BANC*

James W. Hawkins
JAMES W. HAWKINS, LLC
11339 Musette Cir.
Alpharetta, GA 30009
(678) 697-1278

July 16, 2018

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

*Authorities upon which Petitioners chiefly reply are marked with an asterisk.

Statutes

Regulations

Other Authorities

GLOSSARY

ALJ…….FTC Chief Administrative Law Judge D. Michael Chappell

CEO……Chief Executive Officer

CID…….....Civil Investigative Demand

Commission Opinion……Opinion of the Commission, *In re LabMD*, Dkt. No. 9357 (July 28, 2016), stayed sub nom., *LabMD v. FTC*, No. 16-16270-D (11th Cir. Nov. 10, 2016)(SA055-067)

"FTC" or "Commission"…….Federal Trade Commission

JA……..Joint Appendix

OGR Report……..……..STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 113TH CONG., TIVERSA, INC.:WHITE KNIGHT OR HIGH-TECH PROTECTION RACKET (2015), attached as exhibit RX 644 to Respondent LabMD, Inc.'s Motion to Admit Select Exhibits, *available at* https://www.ftc.gov/system/files/documents/cases/150612labmdmtn.pdf#page=175

RB…….Plaintiffs-Appellees' Response Brief

SA……..……..Supplemental Appendix

RULE 35 STATEMENT

This appeal involves questions of exceptional importance regarding qualified immunity for federal employees who retaliate against private citizens when they exercise their First Amendment rights to criticize the government. In addition, the panel decision directly conflicts with authoritative decisions of the Eleventh Circuit Court of Appeals in Petitioner LabMD Inc.'s appeal of a Federal Trade Commission cease and desist order. The appeal is also of exceptional importance because the panels' factual determination that a single file found by one company in 2008 after billions of searches on a peer-to-peer network was "publicly available" has detrimental ramifications for cybersecurity, cybercriminal prosecutions and privacy.

Appellants Sheer and Yodaiken violated LabMD, Inc. ("LabMD") and Daugherty's First Amendment rights when they retaliated against Daugherty and his company for Daugherty's criticism of them and the Commission in his book, *The Devil Inside the Beltway*. They retaliated by misrepresenting critical facts to the Commission in a deliberate and successful effort to cause the Commission to authorize an enforcement action against LabMD. The trial court found that Sheer and Yodaiken's violations of LabMD and Daugherty's "First Amendment rights to criticize the actions of the federal government without fear of government retaliation are as clearly established as can be…." JA 107.

Sheer and Yodaiken argued for the first time on appeal that they did not violate a clearly established right because the Commission would have authorized an

enforcement action even if Sheer and Yodaiken's recommendations were not laced with lies. The panel agreed, believing the Commission had an alternative cause to file an enforcement action against LabMD. Op. 11. The panel also agreed with Sheer and Yodaiken's argument, also made for the first time on appeal, that a LabMD computer file was "publicly available" on peer-to-peer networks, Op. 8, despite the fact that the only company that took the file conducted over *300 billion searches* before locating it. *See*, *infra*, n. 3 and 4. There are no allegations in the complaint, there is no evidence in the record and there is no basis in the technology at issue to conclude that LabMD's file was ever publicly available.

After Sheer and Yodaiken's lies were revealed at trial by a whistleblower, the Commission (1) withdrew its reliance on Sheer and Yodaiken's fabricated evidence of consumer injury; (2) changed its theory of the case; (3) argued that LabMD's file was still publicly available, JA 79; and, (4) because there was no longer any evidence of consumer injury, proceeded with a contorted interpretation of 15 U.S.C. § 45(n) that "substantial injury" includes hypothetical and intangible injuries. The Commission took the very alternative path the panel held was available to the Commission – the same path for which the Eleventh Circuit specifically found was not available because the Commission's interpretation of "substantial injury" under 15 U.S.C. § 45(n) was unreasonable and not entitled to *Chevron* deference. *LabMD, Inc. v. FTC*, 678 F. App'x 816, 820 (11th Cir. 2016). SA 61-62.

Five days after the panel's decision, the Eleventh Circuit gave an additional reason why the Commission and the panel's alternative path was not available to the Commission. The court held that the Commission's cease and desist order against LabMD is unenforceable because it does not direct LabMD to cease committing an unfair act or practice within the meaning of 15 U.S.C. § 45(a). *LabMD, Inc. v. FTC*, 891 F.3d 1286, 1288 (11th Cir. 2018). In that same decision, the Eleventh Circuit underscored another problem with the panel's decision. The court held that the reason for an enforcement action must be supported by clear and well-established policies found in the Constitution, statutes or common law, none of which were cited by the panel to support the panel's view that the Commission had an alternative cause to prosecute LabMD. *Id.*, 891 F.3d at 1295.

The panel decision directly and irreconcilably conflicts with holdings of the Eleventh Circuit and will have unfortunate consequences for cybersecurity, cybercrime prosecutions and privacy.

FACTS

From at least 2001 through approximately January 2014, LabMD operated as a small, medical services company providing doctors with cancer-detection services. JA 4, ¶10.[1] In May 2008, Tiversa, a self-described cybersecurity company started and led by a chiropractor, contacted LabMD to inform it that a LabMD file was available through LimeWire. JA 5, ¶ 17; JA 13-14, ¶ 56-58. The file was a 1,718-page document containing personal information on approximately 9,300 patients (the "1718 File").[2] JA 12, ¶ 48. Tiversa told LabMD that its patented technology and forensic experts had determined that the 1718 File was being searched for on peer-to-peer networks and that the 1718 File had spread across those networks. JA 13, ¶ 55. Tiversa claims that it has "patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day." JA 5-6, ¶ 19; JA 13, ¶ 51. Thus, while the 1718 File and LimeWire were on the same LabMD computer between July 2007 and May 2008,[3] Tiversa

[1] The panel decision incorrectly describes LabMD as a "medical-records company." Op. 2. LabMD has never been a medical records company. LabMD was always a medical laboratory.

[2] The panel decision incorrectly describes this document as "patient records." Op. 2. The 1718 file is an "insurance aging report [that] allegedly contained personal information, such as names, dates of birth, Social Security numbers ("SSNs"), current procedural terminology ("CPT") codes, and health insurance company names, addresses, and policy numbers for approximately 9,300 patients of LabMD's physician clients." SA 2.

[3] *LabMD*, 891 F.3d at 1289 n. 6.

performed over *300 billion searches*[4] before it located the 1718 File on February 25, 2008. JA 12, ¶ 49.

Immediately after Tiversa's call, LabMD investigated and determined that, unbeknownst to LabMD, LimeWire was installed on a LabMD computer that contained the 1718 File. LabMD removed the application right away. JA 13, ¶ 52. Contrary to LabMD policy, LimeWire was installed on that computer sometime in 2005. *LabMD* 891 F.3d at 1289.

There are significant practical and technological distinctions between a file being "available" via LimeWire and a file being "publicly available." Several of these were intentionally set forth in the Complaint in order to explain this important difference. Peer-to-peer networks do not use Google or similar search engines. Users cannot search for files using words or other data contained in the files. JA 11, ¶ 45. Peer-to-peer networks are only capable of searching for filenames. *Id.* The filename of the 1718 File was "insuranceaging_6.05.071.pdf." JA 12, ¶ 50. The only way for a user to locate the 1718 File through LimeWire was to have used the highly unusual search terms "insuranceaging" or "6.05.071." JA 30, ¶133. In addition, in order for a search on a peer-to-peer network to successfully find a file, both the computer searching the file and the computer sharing the file have to be relatively close to each other on the

[4] August 1, 2007 to February 25, 2008 = 208 days x 1.8 billion daily searches = 374 billion searches.

network. This is because peer-to-peer networks are designed to limit the range of searches because "the network is so large that having any search reach every single computer on the network would quickly consume too many network resources, leaving individual computers potentially overloaded and leaving little bandwidth for other purposes." *See* Expert Report of Adam Fisk at 4 and 15, attached as Exhibit 34 to Respondent LabMD, Inc.'s Application for Stay of Final Order Pending Review By a United States Court of Appeals, *available at* https://www.ftc.gov/system/files/documents/cases/160830labmdstayapplication.pdf. Thus, the chance that anyone would ever have searched for or found the 1718 File was extremely remote, JA 12, ¶ 50, as demonstrated in the fact that it took Tiversa over 300 billion searches before it located the 1718 File. Only Tiversa would ever have found the 1718 File. JA 13, ¶ 51. There are no allegations in the complaint, there is no undisputed evidence in the record and there is no basis in the technology at issue to make these allegations implausible.

On January 19, 2010, LabMD received a letter from Sheer stating that the FTC was "conducting a non-public inquiry into LabMD's compliance with federal law governing information security." The letter states, "According to information we have received, a computer file (or files) from your computer network *is available* to users on a peer-to-peer file sharing ("P2P") network (hereinafter, "P2P breach")." (emphasis added). This was not true. Sheer knew that LabMD found and removed the offending software the day Tiversa contacted LabMD in 2008. JA 25, ¶ 115. It later became

evident why Sheer misrepresented the evidence to LabMD – there was no plausible reason for Sheer, Yodaiken and the FTC to investigate LabMD - the 1718 File was not spreading anywhere and there was no substantial injury as required by 15 U.S.C. § 45(n).

On July 19, 2013, Daugherty posted a trailer on the internet for *The Devil Inside the Beltway*, a book he had written about the ordeal he and his company suffered with Sheer, Yodaiken and others at the FTC. The trailer referred to the FTC's actions as an "abusive government shakedown" and explained that his book would "blow the whistle" about how "the Federal Trade Commission began overwhelming … [LabMD, a] small business, a cancer detection center, with their abusive beltway tactics." The trailer was especially critical of Sheer. JA 29, ¶¶ 131. On July 22, 2013, just three days after the trailer for *The Devil Inside the Beltway* was posted on the internet, and almost five months after the Commission's statute of limitations for filing an enforcement action expired,[5] Sheer told a LabMD attorney that he and his staff recommended an enforcement action against LabMD. JA 30, ¶ 132. Sheer had no obligation to tell LabMD anything but he wanted to send a loud and clear message that he would not tolerate Daugherty's criticisms.

In order to establish "substantial injury" as required by 15 U.S.C. § 45(n), Sheer and Yodaiken relied exclusively on Tiversa's evidence that it found the 1718 File

[5] *See* 28 U.S.C. § 2462.

spreading through peer-to-peer networks. This evidence was later proven to be fabricated. JA 31, ¶ 133; JA 79.

Sheer and Yodaiken knew from their collusion with Tiversa, including their agreement that Tiversa would create a sham corporation, The Privacy Institute, to avoid serving a CID on Tiversa and to allow Tiversa to secretly funnel hand-picked documents to the FTC, that Tiversa's evidence was fraudulent. JA 2, ¶ 1; JA 15, ¶ 66-72; JA 18-25, ¶ 82-113; JA 26, ¶ 118-120; JA 27-28, ¶ 124-125; JA 30-31, ¶ 133; JA 32, ¶ 139-40; JA 34, ¶ 146; OGR Report at 4, 54-56, 58-62 and 72. Sheer and Yodaiken knew that without Tiversa's evidence of spread, the Commission would not authorize an enforcement action against LabMD because without evidence that LabMD's file was spreading through cyberspace, "substantial injury" was only hypothetical and hypothetical consumer injury does not satisfy the requirements of 15 U.S.C. § 45(n). *LabMD*, 678 F. App'x at 819-20.

On August 28, 2013, the Commissioners, relying upon Sheer and Yodaiken's misrepresentations, voted unanimously (4-0) to file an administrative enforcement action against LabMD. JA 31, ¶ 133. The Commissioners would not have authorized the enforcement action but for Sheer and Yodaiken's refusal to tell the Commissioners that the 1718 File was hacked by Tiversa, that no one else ever searched for, saw or took the file and that the file never spread on any peer-to-peer network. JA 27, ¶ 124; JA30-31, ¶ 133.

During trial, a whistleblower testified under criminal immunity that Sheer, Yodaiken and the Commission's evidence regarding consumer injury was fabricated. JA 37, ¶ 151. The whistleblower admitted taking the 1718 File directly from a LabMD computer[6] and, at the direction of Tiversa's CEO, manipulated Tiversa's Data Store to make it appear that the 1718 File had been found at multiple IP addresses, including IP addresses of known identity thieves, and fabricated a list of those IP addresses, which Sheer introduced into evidence as CX0019. JA 34, ¶ 146. The Commission admits that "the testimony of Robert Boback, CEO of Tiversa, was not credible or reliable. In particular, we agree that Mr. Boback's assertion that Tiversa had gathered evidence showing that the 1718 file had spread to multiple Internet locations by means of LimeWire was false and that the document that purported to list Internet locations where the 1718 file had been found (CX0019) was unreliable." JA 79 (record references omitted). The whistleblower's testimony led the Commission to withdraw all reliance upon the fabricated evidence and change its theory of the case from one allegedly involving "substantial injury" to one involving hypothetical consumer injury. SA 7 and 9.

The whistleblower's revelations also resulted in a parallel congressional investigation into the FTC's close-knit relationship with Tiversa, JA 34, ¶¶147-49, which culminated in a 93-page report shedding light on Sheer's unusual interactions

[6] Tiversa's theft of the 1718 File was a felony under 42 U.S.C. § 1320d-6 (criminal violations for obtaining individually identifiable health information).

with Tiversa. *See* STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 113TH CONG., TIVERSA, INC.:WHITE KNIGHT OR HIGH-TECH PROTECTION RACKET (2015) attached as exhibit RX 644 to Respondent LabMD, Inc.'s Motion to Admit Select Exhibits, available at https://www.ftc.gov/system/files/documents/cases/150612labmdmtn.pdf#page=175. ("OGR Report"). According to the OGR Report: "*The reason for forging the IP addresses* [from which Tiversa claimed it found the 1718 File], according to the whistleblower, *was to assist the FTC* in showing that P2P networks were responsible for data breaches that resulted in likely harm[.]" OGR Report at 71 (emphasis added).

On November 13, 2015, the ALJ dismissed the government's complaint finding, *inter alia*, that "the record in this case contains no evidence that any consumer whose Personal Information has been maintained by LabMD had suffered any harm as a result of LabMD's alleged failure to employ "reasonable" data security for its computer networks," SA 33; JA 36, ¶ 151, and "fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case." SA 9; JA 35, ¶ 151.

In July 2016, the FTC reversed the ALJ's decision. The Commission held that, contrary to the ALJ's decision, the evidence showed that Section 5(n)'s "substantial injury" prong was met in two ways: the unauthorized disclosure of the 1718 File itself

caused intangible privacy harm, and the mere exposure of the 1718 File on LimeWire likely caused substantial injury. JA 62, 68.

Less than three months after the lower court's denial of Sheer and Yodaiken's motion to dismiss, the FTC promulgated *Bivens* indemnity for its employees. *See* 82 Fed. Reg. 30,966 (June 13, 2017).

ARGUMENT

In *Mt. Healthy City Sch. Dist. Bd. of Educ. v. Doyle*, 429 U.S. 274 (1977), cited in *Hartman v. Moore*, 547 U.S. 250, 256 (2006), the Court held that in a case involving qualified immunity, the burden is properly placed upon a plaintiff to show that his conduct was constitutionally protected, and that this conduct was a "substantial factor" or "motivating factor" causing harm. *Id.* 429 U.S. at 287. Once that burden is carried, the defendant must show by a preponderance of the evidence that it would have reached the same decision even in the absence of the protected conduct. *Id.* In the recent case of *Lozman v. City of Riviera Beach*, 138 S. Ct. 1945 (2018), the Court noted that qualified immunity cases involving retaliation for protected speech, *Mt. Healthy* applies in the civil context and *Hartman* applies in the criminal context. *Id.*, 138 S. Ct. at 1947.

Under *Mt. Healthy*, LabMD and Daugherty only had to plead that the protected speech was a substantial or motivating factor that caused the Commission to authorize the enforcement action. They did: "[t]he FTC Commissioners would not have authorized the Enforcement Action if Sheer and Yodaiken had been truthful and forthcoming with the facts [including, *e.g.*, that Tiversa had manufactured evidence to make it appear that the 1718 File had proliferated on peer-to-peer networks]," JA 30-31, ¶ 133. This is an allegation that this Court must take as true. *Vila v. Inter-American Inv. Corp.*, 570 F.3d 274, 278 (D.C. Cir. 2009).

The panel's conclusion that the Commission had an alternative cause to file an enforcement action against LabMD is wrong for several reasons. LabMD and Daugherty *vehemently* deny that the 1718 File was ever "publicly available" on peer-to-peer networks. They denied that allegation in their complaint, JA 25, ¶ 115, and they specifically denied in their response brief that the file was available to users on peer-to-peer networks. RB at 5. Indeed, the very reason LabMD and Daugherty made so many allegations regarding the limitations of peer-to-peer technology and the virtual impossibility of anyone ever finding the 1718 File was to show that the 1718 File was never publicly available. With all due respect to the panel, the panel has a fundamental misunderstanding of the technology at issue and has failed to construe the allegations in the complaint in favor of LabMD and Daugherty. On a motion to dismiss, this Court must "accept[] as true all of the factual allegations contained in the complaint and draw[] all inferences in favor of the nonmoving party." *Bowman v. Iddon*, 848 F.3d 1034, 1039 (D.C. Cir. 2017) (quoting *Autor v. Pritzker*, 740 F.3d 176, 179 (D.C. Cir. 2014) (citation and internal quotation marks omitted)). "[A] well pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable, and 'that a recovery is very remote and unlikely.'" *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007) (citing *Scheuer v. Rhodes*, 416 U.S. 232, 236 (1974) (a well-pleaded complaint may proceed even if it appears "that a recovery is very remote and unlikely").

There is no Google searching on peer-to-peer networks. The panel's factual determination that the 1718 File was "publicly available" is not founded in technology

and is belied by the allegations in the Complaint that (1) peer-to-peer networks are only capable of searching for filenames, JA11, ¶ 45; (2) the only way for a user to locate the 1718 File was to have used the highly unusual search terms "insuranceaging" or "6.05.071," JA 30, ¶133; (3) the chance that anyone would ever have searched for or found the 1718 file was extremely remote, JA 12, ¶ 50; (4) it took Tiversa over 300 billion searches before locating the 1718 File; (5) only Tiversa, with its "patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day" and its cadre of highly experienced professional hackers, would ever have found the 1718 File, JA 13, ¶ 51; and (6) Tiversa's theft of the 1718 File was a violation of 42 U.S.C. § 1320d-6 (criminal violations for obtaining individually identifiable health information), JA 5, ¶ 13. By analogy, under 18 U.S.C. § 1708, it is a felony to steal or take any letter, postal card, package, bag or mail from a collection box or other authorized depository of mail matter. Mail deposited in millions of U.S. mailboxes every day is "available" to anyone but is not considered "publicly available" despite the ease with which mail can be taken from many of those boxes.

The panel's view that the 1718 File was publicly available also conflicts with the finding of another federal court that concluded whether or not the 1718 File was publicly available is not suitable for resolution on a motion to dismiss. In *LabMD, Inc. v. Tiversa Holding Corp.*, Civil Action No. 15-92, 2016 U.S. Dist. LEXIS 140245, at *17 (W.D. Pa. Oct. 7, 2016), the court found that "[e]ven if such information was technically accessible via inadvertent file sharing…, it was, at a minimum, not legally available to

the public." The court concluded that "[b]ecause the meaning of 'publicly available,' is subject to interpretation, the Court cannot say that LabMD cannot maintain a defamation claim as to Defamatory Statement 16." *Id.*

The panel cited no authority for its proposition that the installation of LimeWire in 2005 or the inadvertent placement of the 1718 File on a computer with a LimeWire application in 2007 demonstrates cause for an enforcement action. In *LabMD*, 891 F.3d at 1295, the court held that "the Commission must find the standards of unfairness it enforces in 'clear and well-established' policies that are expressed in the Constitution, statutes, or the common law." The panel erred as a matter of law because there is no authority for the Commission to have filed an enforcement action against LabMD without evidence of substantial injury as required by 15 U.S.C. § 45(n).

The panel's finding that the 1718 File was publicly available has severe and dangerous consequences for cybersecurity, cybercriminal prosecutions and privacy. Under the ruse that the files were "publicly available," Tiversa has admitted to searching for and downloading confidential, privileged and classified documents including troop movements, Pentagon server, router and IP information, classified files of multiple foreign governments (including allies), Justice Stephen Breyer's social security number, cockpit schematics for the President's Marine One helicopter, attorney-client privileged material, customer bank statements, individual tax returns, credit reports, credit card numbers, medical records, social security numbers, drivers' license numbers and user ids and passwords. A ruling that these files were legally found on a peer-to-peer

network because they were "publicly available" may strip them of their confidential, private, privileged, protected or classified status. In addition, cybercriminals who use technological back doors to enter and take such documents from unsuspecting computer users will cite the panel's decision as a defense in response to criminal charges under 18 U.S.C. § 793 (Espionage Act - Unlawful Gathering and Transmitting of Defense Information), 18 U.S.C. § 798 (Espionage Act - Illegal Disclosure of Classified Information), 18 U.S.C. § 1924 (Unlawful Removal and Retention of Classified Information), 18 U.S.C § 1832 (Economic Espionage Act - Theft of Trade Secrets), 18 U.S.C. § 2511 (Interception and Disclosure of Electronic Communications), 18 U.S.C. § 2701 (Unlawful Access to Stored Communications) and 42 U.S.C. § 1320d-6 (Unlawful Possession and Use of Personal Health Information).

Virtually no online computer is immune from vulnerabilities that allow hackers, like Tiversa, to access and take documents that were never intended to be shared with others. In this case, the Commission had no plausible reason to investigate, had no business cavorting with and using evidence from a profit-motivated shakedown artist and certainly no reason to file an enforcement action. As an Eleventh Circuit panel explained to FTC's counsel at oral argument, "[T]he aroma that comes out of the investigation of this case is that Tiversa was shaking down private industry with the help of the FTC," and further noted Tiversa's "falsifications to the Commission." RB 18. The court understood that there was no authority for the Commission to pursue an enforcement action without evidence of consumer injury when it stated to the

Commission's counsel that it "should have become obvious after you - after the evidence collapsed and your - and complaint counsel couldn't go any further." RB 19.

Finally, the technologies at issue in this case are far too complex for an appellate court to draw factual conclusions, especially with a 2018 perspective applied to how those technologies worked between 2005 and 2008.

CONCLUSION AND REQUESTED RELIEF

For the foregoing reasons, the Court should grant panel rehearing. If panel rehearing is not granted, the Court should grant rehearing *en banc*.

Dated: July 16, 2018

Respectfully submitted,

JAMES W. HAWKINS, LLC

/s/ James W. Hawkins
James W. Hawkins
Georgia State Bar No. 338767
JAMES W. HAWKINS, LLC
11339 Musette Circle
Alpharetta, GA 30009
V: 678-697-1278
F: 678-540-4515
jhawkins@jameswhawkinsllc.com

Attorney for Petitioners

CERTIFICATE OF COMPLIANCE

This Petition complies with the type-volume limit of Fed. R. App. P. 40(b)(1) because, excluding the parts of the petition exempted by Fed. R. App. P. 32(f), the Petition contains 3,899 words. This Petition also complies with the typeface and type-style requirements of Fed. R. App. P. 32(a)(5)-(6) because it was prepared using Microsoft Word for Mac Version 16.14.1 in Garamond 14-point font, a proportionally spaced typeface.

/s/ James W. Hawkins
James W. Hawkins

ADDENDUM

ADDENDUM: PANEL OPINION

United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued January 9, 2018 Decided June 1, 2018

No. 17-5128

MICHAEL J. DAUGHERTY AND LABMD, INC.,
APPELLEES

v.

ALAIN H. SHEER, IN HIS INDIVIDUAL CAPACITY AND RUTH T. YODAIKEN, IN HER INDIVIDUAL CAPACITY,
APPELLANTS

DOES 1-10, IN THEIR INDIVIDUAL CAPACITIES,
APPELLEES

Appeal from the United States District Court
for the District of Columbia
(No. 1:15-cv-02034)

Tyce R. Walters, Attorney, U.S. Department of Justice, argued the cause for appellants. With him on the briefs were *Jessie K. Liu*, U.S. Attorney, and *Mark B. Stern*, Attorney.

James W. Hawkins argued the cause and filed the brief for appellees.

Patrick J. Massari and *Michael Pepson* were on the brief for *amicus curiae* Cause of Action Institute in support of plaintiffs-appellees.

Before: PILLARD and WILKINS, *Circuit Judges*, and SENTELLE, *Senior Circuit Judge*.

Opinion for the Court filed by *Circuit Judge* WILKINS.

WILKINS, *Circuit Judge*: This case requires us to decide whether two Federal Trade Commission attorneys are immune from suit for their conduct during an enforcement action against a medical-records company after the company's CEO publicly criticized the FTC about their investigation, where the company's data-security practices made patient records available over public file-sharing. Because "qualified immunity protects all but the plainly incompetent or those who knowingly violate the law," *Mullenix v. Luna*, 136 S. Ct. 305, 308 (2015) (internal quotation marks omitted), the answer is yes. Even if the FTC attorneys sought to retaliate for the public criticism, their actions do not violate any clearly established right absent plausible allegations that their motive was the but-for cause of the Commission's enforcement action.

I.

LabMD, Inc. is a small medical-services company in Fulton County, Georgia, owned by Michael Daugherty.[1] LabMD maintained personal information about thousands of patients, including information covered by the Health

[1]This factual background relies on the allegations in the Complaint: we assume the truth of these allegations when reviewing the denial of a motion to dismiss. *Vila v. Inter-Am. Inv., Corp.*, 570 F.3d 274, 278 (D.C. Cir. 2009).

Insurance Portability and Accountability Act of 1996 ("HIPAA").

In May 2008, data-security company Tiversa Holding Corporation notified LabMD that Tiversa located a LabMD PDF file with personal information about 9,300 patients on LimeWire, a peer-to-peer file-sharing application. Tiversa was able to access and download this file, known as the "1718 File," through its data-monitoring technologies that run a prodigious number of searches across file-sharing networks. Tiversa also informed LabMD that the 1718 File had "spread," meaning that other users searched for and downloaded the file on various peer-to-peer networks. LabMD determined that the 1718 File was on LimeWire because the application was installed on a LabMD billing computer, and the company removed LimeWire immediately. LabMD employees searched for the 1718 File on other networks, but did not find it. Plaintiffs-Appellees allege that Tiversa's actions were a sales tactic to attempt to persuade LabMD to purchase Tiversa's data-breach-remediation services.

Enter the FTC. On January 19, 2010, LabMD CEO Daugherty received a letter from Alain Sheer, an FTC enforcement attorney, informing LabMD that the FTC was investigating LabMD's information-security practices, because "[a]ccording to information [they] ha[d] received, a computer file (or files) from your computer network is available to users on a peer-to-peer file sharing ('P2P') network." Compl. ¶ 115. According to Plaintiffs-Appellees, Sheer knew about the 1718 File only because Tiversa contacted the FTC to suggest an investigation, another Tiversa strategy for pressuring companies to retain their services.

Over the next three and a half years, FTC attorneys Sheer and Ruth Yodaiken investigated Daugherty and LabMD

regarding the company's data-security practices that allowed the 1718 File to be available on LimeWire. During this period, Daugherty publicly criticized the FTC, Sheer, and Yodaiken regarding the conduct of the investigation. On September 7, 2012, the Atlanta Business Chronicle quoted Daugherty describing the FTC's investigation as "a fishing expedition" that was "beating up on small business." Compl. ¶ 128. An FTC paralegal downloaded the article and sent it to Sheer, Yodaiken, and others not named. *Id.* ¶ 129. Daugherty and LabMD allege that "[a]fter reading Daugherty's quote, Sheer and Yodaiken ramped up their investigative efforts against Daugherty and LabMD." *Id.* ¶ 130. However, it is not alleged what this "ramp[ing] up" entailed. On July 19, 2013, Daugherty posted on the internet a "trailer" for his book, *The Devil Inside the Beltway*, which details his experience with the FTC investigation into LabMD. Three days later, Sheer informed LabMD's attorney that the investigation team had recommended an enforcement action against LabMD to the Commission, which would make the decision about whether to bring such an action. The Commission voted unanimously to do so on August 28, 2013: the complaint against LabMD alleged that it failed to provide appropriate security for patient information, in violation of Section 5 of the Federal Trade Commission Act ("FTCA").

II.

LabMD continues to defend against the FTC enforcement action, now in federal court. LabMD also filed several cases attacking those proceedings. Each of its three lawsuits seeking to enjoin the FTC has been dismissed. *See LabMD, Inc. v. FTC*, No. 14-cv-810 (N.D. Ga. May 12, 2014); *LabMD, Inc. v. FTC*, No. 13-cv-1787 (D.D.C. Feb. 19, 2014); *LabMD, Inc. v. FTC*, No. 13-15267 (11th Cir. Feb. 18, 2014). This suit for damages against Sheer, Yodaiken, and another FTC attorney in

their personal capacities is LabMD's fourth offensive foray in response to the FTC's enforcement effort.

Defendants moved to dismiss, and the District Court granted the motion with respect to all but the claim that the FTC attorneys Sheer and Yodaiken retaliated against LabMD and Daugherty based on Daugherty's exercise of his First Amendment rights to publicly criticize the government. *See Daugherty v. Sheer*, 248 F. Supp. 3d 272 (D.D.C. 2017). For this particular claim, the District Court framed the allegations as "claiming that Defendants increased the intensity of the investigation in 2012 and 2013, and later in 2013 elevated the matter to an enforcement proceeding following additional public criticism by Daugherty." *Id.* at 285. The District Court concluded that no special factors or alternative remedial scheme precluded a *Bivens* remedy for Plaintiffs-Appellees' First Amendment claims and denied Defendants' qualified-immunity defenses, reasoning that

> Plaintiffs' First Amendment rights to criticize the actions of the federal government without fear of government retaliation are as clearly established as can be, and a serious escalation of an agency's investigation or enforcement against Plaintiffs for publicly criticizing the agency would appear to violate that clearly established constitutional right.

Id. at 290.

Sheer and Yodaiken appealed. We review de novo, and "in reviewing the denial of the motion to dismiss, we take the allegations of the complaint as true." *Vila*, 570 F.3d at 278. "In assessing a claim of qualified immunity, the facts must be taken 'in the light most favorable to the party asserting the injury.'" *Corrigan v. Dist. of Columbia*, 841 F.3d 1022, 1035

(D.C. Cir. 2016) (quoting *Saucier v. Katz*, 533 U.S. 194, 201 (2001)).

III.

"Qualified immunity depends upon the answers to two questions: (1) Did the officer's conduct violate a constitutional or statutory right? If so, (2) was that right clearly established at the time of the violation?" *Jones v. Kirchner*, 835 F.3d 74, 84 (D.C. Cir. 2016). Court have discretion to answer these questions in either order. *Ashcroft v. al-Kidd*, 563 U.S. 731, 735 (2011). Accordingly, "courts may grant qualified immunity on the ground that a purported right was not 'clearly established' by prior case law, without resolving the often more difficult question whether the purported right exists at all." *Reichle v. Howards*, 566 U.S. 658, 664 (2012).

For a right to be clearly established, "existing precedent must have placed the statutory or constitutional question beyond debate." *Reichle*, 566 U.S. at 664 (quoting *al-Kidd*, 563 U.S. at 741). This standard does not "require a case directly on point." *al-Kidd*, 563 U.S. at 741. Regardless of whether a court expressly has declared certain conduct unlawful, a government official is not entitled to qualified immunity where "every 'reasonable official would have understood that what he is doing violates th[e] right.'" *Id.* (quoting *Anderson v. Creighton*, 483 U.S. 635, 640 (1987)). Accordingly, "we look to cases from the Supreme Court and this court, as well as to cases from other courts exhibiting a consensus view – if there is one." *Bame v. Dillard*, 637 F.3d 380, 384 (D.C. Cir. 2011) (citation and quotation marks omitted). The proponent of a purported right has the "burden to show that the particular right in question . . . was clearly established" for qualified-immunity purposes. *Dukore v. Dist. of Columbia*, 799 F.3d 1137, 1145 (D.C. Cir. 2015).

In assessing whether a right is clearly established, courts must mind the Supreme Court's admonishment "not to define clearly established law at a high level of generality." *al-Kidd*, 563 U.S. at 742. This means, for instance, that courts cannot rely on "[t]he general proposition . . . that an unreasonable search or seizure violates the Fourth Amendment." *Id.* Similarly, in the First Amendment context, "the general right to be free from retaliation for one's speech" may be too broad a proposition, not sufficiently "particularized" to make out clearly established law. *Reichle*, 566 U.S. at 665. Again, the touchstone remains whether the "contours of the right are clear to a reasonable officer." *Id.* (quotation marks omitted).

IV.

In their claim now on appeal, Daugherty and LabMD assert that Sheer and Yodaiken violated their rights by prosecuting an enforcement action in retaliation for Daugherty's speech, despite the undisputed data-security breach underlying the FTC's investigation and regardless of ultimate control over the decision to bring a complaint residing with the FTC board. Because no such right was clearly established, Sheer and Yodaiken are immune from this suit.

We first consider the scope of the retaliation that Plaintiffs-Appellees allege. As an initial matter, it is beyond dispute that the FTC enforcement action began long before Daugherty's speech upon which the alleged retaliation purportedly was based – in fact, Daugherty's statements were about the ongoing FTC investigation. Accordingly, we understand Plaintiffs-Appellees' arguments to allege retaliation through Sheer's and Yodaiken's conduct while investigating, recommending, and later prosecuting the FTC enforcement action – not the decision to instigate the investigation in the first place.

We next consider the appropriate level of generality for analyzing whether the right is clearly established. Daugherty and LabMD assert a First Amendment right to be free from the FTC ramping up its enforcement action after Daugherty publicly criticized the FTC. Plaintiffs-Appellees focus on their allegation that "not one single patient suffered harm due to any alleged disclosure of the 1718 file," Appellees' Br. 39, in an attempt to undercut the factual basis for the FTC's action. But this is unpersuasive in light of other facts that are undisputed: Daugherty and LabMD do not deny – nor could they – that the 1718 File was publicly available from a LabMD computer on LimeWire's peer-to-peer network, and that Tiversa was able to access and download the file over that system. The 1718 File contained confidential personal information about approximately 9,300 patients. While the Complaint casts LabMD as the "victim of inadvertent file sharing," Compl. ¶ 48, and Plaintiffs-Appellees argue at length that there was no consumer injury based on the availability of the 1718 File, Plaintiffs-Appellees' own characterization of the facts belies any implication that the FTC's enforcement action was specious. And while Plaintiffs-Appellees take issue with the relationship between Tiversa and the FTC, their allegations that the FTC investigated Tiversa's targets to gin up customers for Tiversa do not controvert the data-security issue underlying the FTC's investigation. Like the fact that the investigation began long before Daugherty's criticism of the FTC and its enforcement team, the undisputed factual basis for the FTC's enforcement action demonstrates a cause for that action – regardless of whether FTC staff also had retaliatory motive based on Daugherty's intervening speech. Our task, then, is to determine whether there is a clearly established right to be free from an enforcement action where retaliatory motive was allegedly present, but was not plausibly alleged to be the but-for cause of the enforcement.

Supreme Court precedent shows that there is no such clearly established right. If anything, the leading cases cut the other way: they show that retaliatory motive does not automatically imbue the conduct in question with an unconstitutional air, where the official's actions have a legitimate basis. In *Crawford-El v. Britton*, the Supreme Court explained that "proof of an improper motive is not sufficient to establish a constitutional violation – there must also be evidence of causation," as well as clarity that the conduct in question violated a right. 523 U.S. 574, 593 (1998). The Court reasoned that the causation element provides a check against the "serious problem" of spurious allegations of improper motive by government officials, notoriously "easy to allege and hard to disprove." *Id.* at 584-85, 592-93.

The same principles found further purchase in *Hartman v. Moore*, where the Court concluded that an absence of probable cause has "powerful evidentiary significance" in any retaliatory-prosecution case and accordingly must be pleaded and proved by the plaintiff. 547 U.S. 250, 261 (2006). The presence or absence of probable cause is especially critical where one official recommends prosecution to a different decision-maker because "the causal connection . . . is not merely between the retaliatory animus of one person and that person's own injurious action, but between the retaliatory animus of one person and the action of another." *Id.* at 262. Although "showing an absence of probable cause may not be conclusive that the inducement [to prosecute] succeeded, and showing its presence does not guarantee that inducement was not the but-for fact in a prosecutor's decision," the question of a proper, alternative basis for a prosecution "will have high probative force" in determining whether an officer's retaliatory motive caused a constitutional injury. *Id.* at 265.

Applying these concepts here, we conclude that Daugherty and LabMD have failed to allege that Sheer and Yodaiken violated any clearly established right. At core, the allegations relate that Sheer and Yodaiken continued an ongoing FTC investigation, based on an undisputed data breach of LabMD's records. Even if the FTC staff were motivated to retaliate against Daugherty and LabMD because of Daugherty's statements criticizing them, Plaintiffs-Appellees have not alleged that any such retaliatory animus actually caused the injury that they assert. They have not alleged that Sheer and Yodaiken retaliated in initiating the inquiry – to the contrary, Daugherty had not yet said the things that purportedly inspired the FTC staff's animosity. They do not contend that the FTC lacked any reason to believe that LabMD violated the FTCA – information about some 9,300 patients in the 1718 File was available publicly from a LabMD computer via LimeWire, although they dispute whether any consumers were harmed by that publication. And while they include a conclusory allegation that Sheer and Yodaiken "ramped up" their investigative efforts in response to Daugherty's public criticism, they nowhere allege causation to "bridge the gap" between that alleged retaliation and the Commission's unanimous vote to proceed with an enforcement action against LabMD. *See Hartman*, 547 U.S. at 263. With these layers of alternative causality separating Sheer's and Yodaiken's conduct from the effect on LabMD and Daugherty, the Defendants-Appellants' allegedly retaliatory conduct during the continuing investigation did not violate Daugherty's and LabMD's clearly established rights. Accordingly, Sheer and Yodaiken are entitled to qualified immunity and need not defend against this suit.

* * *

Because the FTC enforcement action against LabMD had an alternative cause – the undisputed data-security breach by which the 1718 File was publicly available from a LabMD computer – the alleged actions by Sheer and Yodaiken did not violate Daugherty's or LabMD's clearly established rights, even assuming retaliatory motive. Sheer and Yodaiken accordingly are entitled to qualified immunity, and the District Court's decision concluding otherwise is REVERSED.

ADDENDUM: CERTIFICATE AS TO PARTIES, RULINGS AND RELATED CASES

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), the undersigned counsel certifies as follows:

Parties and Amici: Petitioners are Michael J. Daugherty ("Daugherty") and LabMD, Inc. ("LabMD"). Daugherty is the sole shareholder of LabMD. LabMD has no parent, subsidiary or affiliate. LabMD has never issued shares or debt securities to the public.

Respondents are Alain H. Sheer and Ruth T. Yodaiken, in their individual capacities. The district court granted the motion to dismiss as to defendant Carl H. Settlemyer, III, in his individual capacity. Plaintiffs' Complaint also named Does 1-10 as defendants.

Cause of Action Institute filed an *amicus curiae* brief in the above-captioned matter in support of Appellees Michael J. Daugherty and LabMD, Inc.

Rulings Under Review: Petitioners seek rehearing by the panel or, in the alternative, rehearing en banc of the panel's decision in *Daugherty v. Sheer*, 891 F.3d 386 (D.C. Cir. 2018).

Related Case: This case was previously before this Court. *LabMD, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018) is a related case within the meaning of this Court's Rule 28(a)(1)(C), as it involves substantially the same parties and similar issues.

/s/ James W. Hawkins
James W. Hawkins

ADDENDUM: DISCLOSURE STATEMENT

DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and D.C. Circuit Rule 26.1, Petitioners provide the following disclosure:

Petitioners are Michael J. Daugherty ("Daugherty") and LabMD, Inc. ("LabMD"). Daugherty is the sole shareholder of LabMD. LabMD has no parent, subsidiary or affiliate. LabMD has never issued shares or debt securities to the public.

ADDENDUM: CERTIFICATE OF SERVICE

CERTIFICATE OF SERVICE

I hereby certify that on July 16, 2018, I electronically filed the foregoing Petition with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. Participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

/s/ James W. Hawkins
James W. Hawkins