

**NO. 16-16270**  
**IN THE UNITED STATES COURT OF APPEALS**  
**FOR THE ELEVENTH CIRCUIT**

---

**LabMD, Inc.,**  
*Petitioner,*  
**v.**  
**Federal Trade Commission,**  
*Respondent.*

---

**On Petition for Review from the Federal Trade Commission, *In the Matter of***  
***LabMD, Inc.*, FTC Matter/File Number: 102 3099, Docket Number: 9357**

---

**AMICUS CURIAE BRIEF OF EIGHT PRIVACY AND SECURITY LAW**  
**PROFESSORS IN SUPPORT OF RESPONDENT, FEDERAL TRADE**  
**COMMISSION**

---

Michael W. Sobol  
Lief Cabraser Heimann &  
Bernstein, LLP  
275 Battery Street, 29th Floor  
San Francisco, CA 94111-3339  
415.956.1000

Nicholas R. Diamand  
Lief Cabraser Heimann &  
Bernstein, LLP  
250 Hudson Street, 8th Floor  
New York, NY 10013-1413  
212.355.9500

Laura B. Heiman  
Lief Cabraser Heimann &  
Bernstein, LLP  
One Nashville Place  
150 Fourth Avenue, North, Suite 1650  
Nashville, TN 37219-2423  
615.313.9000

**UNITED STATES COURT OF APPEALS  
FOR THE ELEVENTH CIRCUIT**

LabMD, INC.,

Petitioner,

v.

FEDERAL TRADE COMMISSION,

Respondent.

Case File No. 16-16270

FTC Docket No. 9357

**CERTIFICATE OF INTERESTED PERSONS  
AND CORPORATE DISCLOSURE STATEMENT (CIP)**

In compliance with Local Rule 26.1-1 and Local Rule 29(c), the undersigned certifies that no counsel to a party authored this brief in whole or in part nor contributed any funds directly or indirectly for this brief's preparation, and that no person other than the amici curiae contributed any funding for the preparation of this brief. Additionally, the following individuals or entities may have an interest in the outcome of this matter:

Bamberger, Kenneth A.—*Amicus Curiae*

Black, David L.—*Amicus Curiae*

Boies, Schiller & Flexner LLP—Counsel for *Amicus Curiae* NTSC

Cause of Action—Counsel for LabMD before FTC and counsel for Amici  
Curiae David Black *et al.*

(listed in LabMD's certificate solely as counsel for LabMD)

Chamber of Commerce of the United States of America—*Amicus Curiae*

Consovoy McCarthy Park PLLC—Counsel for *Amicus Curiae* Chamber of  
Commerce

Consovoy, William S.—Attorney, Consovoy McCarthy Park PLLC

Gilbert, Sheldon—Attorney—U.S. Chamber Litigation Center

Gottlieb, Michael J.—Attorney, Bois, Schiller & Flexner, LLP

Green, Bruce G.—*Amicus Curiae*

Hader, Joan E.—*Amicus Curiae*

Hartzog, Woodrow—*Amicus Curiae*

Hill, Brian E.—*Amicus Curiae*

Hitt, Warren—*Amicus Curiae*

Hoofnagle, Chris Jay—*Amicus Curiae*

Hutchins, John P.—Attorney, LeClairRyan

International Center for Law & Economics (“ICLE”)—*Amicus Curiae*

Kilpatrick Townsend & Stockton LLP—Counsel for *Amicus Curiae* NFIB  
and former counsel for LabMD

LeClairRyan—Counsel for Amici Curiae ICLE and TechFreedom

Lehotsky, Steven P.—Attorney, U.S. Chamber Litigation Center

Lieff Cabraser Heimann & Bernstein, LLP—Sobol, Michael W.; Diamand,  
Nicholas R.; Heiman, Laura B. (counsel for *Amici Curiae* Kenneth A.  
Bamberger, Woodrow Hartzog, Chris Jay Hoofnagle, William  
McGeeveran, Deirdre K. Mulligan, Paul Ohm, Daniel J. Solove, and  
Peter Swire).

Manne, Geoffrey A.—Attorney, International Center for Law & Economics

McGeeveran, William—*Amicus Curiae*

Miliefsky, Gary—*Amicus Curiae*

Mulligan, Deirdre K. —*Amicus Curiae*

Nabors, William L.—*Amicus Curiae*

National Federation of Independent Business Small Business Legal Center  
 (“NFIB”)—*Amicus Curiae*

National Technology Security Coalition (“NTSC”)—*Amicus Curiae*

Norris, Cain M.—Attorney, Bois, Schiller & Flexner, LLP

Ohlhausen, Maureen K.—Acting Chairman and Commissioner, FTC (new  
 title)

Ohm, Paul—*Amicus Curiae*

Park, John. J., Jr.—Attorney, Strickland Brockington Lewis, LLP.

Park, Michael H.—Attorney, Consovoy McCarthy Park PLLC

Ramirez, Edith—Commissioner and former Chairwoman, FTC (new title)

Ronald L. Raider—Attorney, Kilpatrick Townsend & Stockton LLP

Ross, Jr., Robert R.—*Amicus Curiae*

Singleton, Burleigh L.—Attorney, Kilpatrick Townsend & Stockton LLP

Solove, Daniel J. —*Amicus Curiae*

Stout, Kristian—Attorney, International Center for Law & Economics

Strickland Brockington Lewis, LLP—Counsel for *Amicus Curiae* Gary  
 Miliefsky

Swire, Peter—*Amicus Curiae*

TechFreedom—*Amicus Curiae* (before FTC and this Court) (listed in  
 LabMD’s certificate solely as *Amicus Curiae* before agency)

Todd, Kate Comerford—Attorney, U.S. Chamber Litigation Center

U.S. Chamber Litigation Center—Counsel for *Amicus Curiae* Chamber of  
Commerce

Dated: February 16, 2017

Respectfully submitted,

/s/ Laura B. Heiman

Laura B. Heiman

lheiman@lchb.com

LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLP

One Nashville Place

150 Fourth Avenue North, Suite 1650

Nashville, TN 37219-2423

Telephone: 615.313.9000

Facsimile: 615.313.9965

## **TABLE OF CONTENTS**

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT (CIP) .....	C-1
TABLE OF CONTENTS .....	i
TABLE OF AUTHORITIES .....	iii
STATEMENT OF INTEREST .....	1
STATEMENT OF THE ISSUES .....	1
SUMMARY OF ARGUMENT .....	2
ARGUMENT .....	3
I. FTC ENFORCEMENT IN COMBINATION WITH OTHER AGENCY ACTIVITIES FOSTERS CORPORATE INNOVATION IN PRIVACY PROTECTION .....	4
A. The FTC Works Extensively and Collaboratively with Stakeholders Addressing Evolving Areas of Consumer Privacy and Security .....	6
B. The FTC’s Strategic Use of its Unfairness Authority Encourages and Supports Consumer Privacy Protection .....	9
C. Scholarship on Regulatory Governance Supports the FTC’s Broad Discretion with Respect to Unfairness Enforcement in the Data Privacy Sphere .....	12
II. THE TYPES OF INJURY AT ISSUE IN THIS AND OTHER DATA SECURITY CASES FALL SQUARELY WITHIN THE PREVENTATIVE ENFORCEMENT POWER THAT CONGRESS GRANTED THE FTC WITH RESPECT TO ACTS OR PRACTICES LIKELY TO CAUSE SUBSTANTIAL INJURY TO CONSUMERS .....	17
III. HIPAA DOES NOT PREEMPT THE FTC’S AUTHORITY .....	23
A. The Text and History of HIPAA Provide No Basis for Finding that the Statute Preempts Section 5 of the FTC Act .....	24
B. Congress has Continually Expanded the Entities that Can Protect Health Privacy and Security .....	25
C. The History of the FTC Does Not Support Preemption .....	26
CONCLUSION .....	29

ADDENDUM: IDENTITY OF AMICI CURIAE .....	i
--	---

## **TABLE OF AUTHORITIES**

### **Cases**

<i>Federal Trade Commission v. D-Link Corp. et al</i> , 3:17-CV-00039, (N.D. Cal., Jan 5, 2017) .....	27
<i>FTC v. Ken Roberts Co.</i> , 276 F.3d 583 (D.D.C. 2001) .....	33, 34
<i>GeorgiaCarry.Org, Inc. v. U.S. Army Corps of Eng’rs</i> , 788 F.3d 1318 (11th Cir. 2015) .....	5
<i>In re Eli Lilly &amp; Co.</i> , 133 F.T.C. 763 (2002) .....	20
<i>In the Matter of Designware LLC</i> , Decision and Order, FTC File No. 1123151, Docket No. C-4390, Apr. 11, 2013 .....	26
<i>In the Matter of HTC America Inc.</i> , FTC File No. 1223049, Docket No. C-4406, June 25, 2013 .....	27
<i>Thompson Med. Co. v. FTC</i> , 791 F.2d 189 (D.C. Cir. 1986) .....	34

### **Statutes**

15 U.S.C. § 45 .....	1, 19, 27
15 U.S.C. § 7711 .....	26
15 U.S.C. §§ 13c, 45(a)(2) (2012) .....	27
42 U.S.C. § 1320d-5(d) (2012) .....	26
42 U.S.C. § 17934(a), (c) (2012) .....	25
CAN SPAM Act of 2003. Pub. L. 108-187 .....	26
Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501– 6505 (2012) .....	26
Gramm-Leach-Bliley Act (“GLBA”) .....	26
Pub. L. 104-191 .....	24
Pub. L. No. 111-5, §§ 13001–13424, 123 Stat. 115, 226–79 .....	25

### **Rules**

65 Fed. Reg. 82462, 82481-87 (Dec. 28, 2000) .....	24, 25
68 Fed. Reg. 8334, 8355 (Feb. 20, 2003) .....	24



**Other Authorities**

Chris Jay Hoofnagle, <i>Federal Trade Commission Privacy Law and Policy</i> 224 (2016) .....	18, 20, 21
Daniel J. Solove, <i>A Taxonomy of Privacy</i> , 154 U. Penn. L. Rev. 477, 515 (2006) .....	17, 18
David Thaw, <i>Enlightened Regulatory Capture</i> , 89 Wash. L. Rev. 329, 331 (2014) .....	14
Deirdre K. Mulligan & Fred B. Schneider, <i>Doctrine for Cybersecurity</i> , Dædalus, Fall 2011 .....	15
FTC, <i>Peer-to-Peer File Sharing: A Guide to Business</i> January 2010.....	8
<i>Health Information Privacy: State Attorneys General</i> , U.S. Dep’t Health & Hum. Servs.....	26
Kenneth A. Bamberger & Deirdre K. Mulligan, <i>New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry</i> , 33 Law & Pol’y 477 (2011) .....	12, 13, 15
Kenneth A. Bamberger & Deirdre K. Mulligan, <i>Privacy on the Books and on the Ground</i> , 63 Stan. L. Rev. 247 (2011).....	passim
Kenneth A. Bamberger & Deirdre K. Mulligan, <i>Privacy On the Ground: Driving Corporate Behavior in the United States and Europe</i> , MIT Press, 2015, 190.....	6
Kenneth A. Bamberger, <i>Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State</i> , 56 Duke L.J. 377, 387–88 (2006) .....	13, 14
Memorandum of Understanding Between the Federal Trade Commission and the Food and Drug Administration, 36 Fed. Reg. 18,539, 18,539 (Sept. 16, 1971).....	28
Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013) .....	28
Nathaniel S. Good and Aaron Krekelberg, “Usability and Privacy: A Study of KaZaA P2P File-Sharing” (June 2002) .....	7
Ross Anderson & Tyler Moore, <i>The Economics of Information Security</i> , 314 Science 610 (2006).....	16

<i>Security Check: Reducing Risks to your Computer Systems .....</i>	<i>7</i>
U.S. Department of Health and Human Services. HIPAA for Professionals.....	24
World Privacy Forum, “Medical Identity Theft .....	19
World Privacy Forum, Medical ID Theft a Threat for Anthem Breach Victims, Key Tips, Feb. 6, 2015 .....	19

### **STATEMENT OF INTEREST**<sup>1</sup>

Amici curiae, Kenneth A. Bamberger, Woodrow Hartzog, Chris Jay Hoofnagle, William McGeveran, Deirdre K. Mulligan, Paul Ohm, Daniel J. Solove and Peter Swire are professors of privacy and security law.<sup>2</sup>

All amici, except for Professor Ohm, aver they have not directly or indirectly received financial support from the FTC, nor have their institutions, to amici's knowledge. From September 2012 to June 2013, Paul Ohm served as a Senior Policy Advisor for the FTC's Office of Policy Planning. During that year, the FTC entered into an agreement with his then-employer, the University of Colorado, under the Intergovernment Personnel Act, to cover some of his salary. Professor Ohm did not work on the underlying matter of this case in any capacity.

### **STATEMENT OF THE ISSUES**

Whether the Federal Trade Commission (the "FTC") exceeded its legal authority in finding the data-security practices of Petitioner LabMD, Inc. ("LabMD") "unfair" under Section 5 of the FTC Act, 15 U.S.C. § 45?

---

<sup>1</sup> All parties have consented to the filing of this brief.

<sup>2</sup> A further description of each amicus is included as an addendum to this brief.

## **SUMMARY OF ARGUMENT**

The FTC's requirement that companies implement "reasonable" data security measures rather than directing companies to implement uniform measures drives both corporate innovation and an evolving understanding of best practices to protect consumers' personal information. This amicus brief presents empirical research from academic experts in privacy and security law who have studied corporate decision making about privacy on the frontline. Their interviews of leading chief privacy officers show that the FTC's broad discretion to enforce data security spurs companies to hire information privacy and security specialists who then develop evolving best practices in the face of risks posed by changes in technology and business practices.

Indeed, the FTC's strategic use of its unfairness authority in the data privacy context encourages corporations to develop progressive and dynamic approaches to privacy policies, guided by a consumer-protection metric. The approach incorporates agency flexibility and harnesses state and market forces

The FTC has frequently used its Section 5 authority to curb or prevent disclosure of consumers' confidential medical information in prior health-related enforcement actions. Its finding of injury and substantial risk of injury stemming from LabMD's disclosure of patient medical records here is thoroughly consistent with the FTC precedent. Moreover, the FTC has historically addressed emerging

threats to consumers as industries and technology progress. Those goals continue today as the FTC tackles modern harms and invasions of privacy citizens face today.

LabMD's argument that the Health Insurance Portability and Accountability Act ("HIPAA") implicitly repealed the FTC's Section 5 authority is unsupported by the text of the law, and regulations promulgated under the law, and inconsistent with subsequent Congressional and agency action which has furthered empowered the FTC to address the security of health information and fostered collaboration on rules and enforcement between the U.S. Department of Health and Human Services ("HHS") and the FTC. Moreover, Appellant's argument is inconsistent with how the FTC has operated for nearly a century.

### **ARGUMENT**

The FTC's approach to data privacy enforcement—requiring companies to implement “reasonable” data security measures rather than forcing every company to implement the same one-size-fits-all measures—is driving corporate innovation and an evolving understanding of best practices to protect consumers' personal information. This amicus brief presents empirical research from academic experts in privacy and security law who have studied corporate decision making about privacy on the ground. Their interviews of leading chief privacy officers show that the FTC's broad discretion with respect to data security enforcement is an

important factor spurring companies to hire information security specialists and allow those specialists to develop evolving best practices to address risks to privacy as technology and business practices change. This brief also provides scholarly insight into the types of harms at issue in the data privacy context and the FTC's congressional mandate to address and prevent such harms. Finally, we review the history of Congress' enactment of health privacy protections that both expand the FTC's authority and leave the FTC's Section 5 authority undisturbed.

**I. FTC ENFORCEMENT IN COMBINATION WITH OTHER AGENCY ACTIVITIES FOSTERS CORPORATE INNOVATION IN PRIVACY PROTECTION**

University of California Berkeley Professors, and amici, Mulligan and Bamberger, recently conducted an empirical study into corporate privacy practices, and their results underscore the value of the FTC's approach to unfairness enforcement in the data privacy context—the very same approach at issue in this case. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Books and on the Ground, 63 Stan. L. Rev. 247 (2011) [“Privacy on the Books”]. This Court and others have recognized empirical data, when available, is a valuable tool in assessing the fit between regulatory methods and objectives. *See, e.g., GeorgiaCarry.Org, Inc. v. U.S. Army Corps of Eng'rs*, 788 F.3d 1318, 1328 (11th Cir. 2015).

As explained by Bamberger and Mulligan, the FTC's enforcement actions are an important component of a broad suite of FTC privacy activities that have spurred improvements in corporate privacy programs. The FTC has leveraged its doctrinal latitude and institutional breadth to facilitate a dialogue about corporate data practices, consumer understanding and expectations, and consumer harms. The FTC's governance style has been open and collaborative. It has convened "Advisory Committees and workshops, request[ed] and issu[ed] reports, work[ed] with and plac[ed] pressure on industry to develop self-regulatory codes of conduct and transparent privacy practices, and safeguard personal information." Bamberger & Mulligan, Privacy on the Books at 286. Against this backdrop of public processes that "exploit market, corporate, and advocacy capacity to develop collective understanding of risk, and solutions to future privacy problems," *id.* at 313, the FTC has made thoughtful and strategic use of its enforcement authority. In doing so, the FTC's approach has "avoid[ed] both the shortcomings of static, top-down, command-and-control regulatory approaches and the ways in which reliance on bottom-up self-regulation alone can subvert public goals by private interests." *Id.* at 313. Its enforcement actions, in particular, have encouraged responsible companies to invest in internal privacy and security professionals and increased the power and resources these professionals have to evolve and strengthen firm privacy practices.

**A. The FTC Works Extensively and Collaboratively with Stakeholders Addressing Evolving Areas of Consumer Privacy and Security**

To advance the privacy and security of consumer data the FTC has hosted over thirty-five workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security, and issued over fifty reports reflecting its own research and work presented and discussed in these forums. Federal Trade Commission, Privacy and Data Security Update 2016.<sup>3</sup> These workshops have covered a wide range of technology—Internet of Things, Mobile Payments, Radio Frequency Identification—and provide important opportunities for shared understandings of the technology, risks to privacy and security, and policy and technical choices to address them. As Bamberger and Mulligan note, the “FTC’s methods produced a detailed public record of factual data about privacy-impacting technologies and related business practices, and how these practices in turn related to consumers’ expectations and privacy concerns.” Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy On the Ground: Driving Corporate Behavior in the United States and Europe, MIT Press, 2015, 190. As part of its privacy work, the FTC has released numerous guidance documents for businesses identifying general strategies for information security programs and at times addressing specific risks. In 2003 the FTC released *Security*

---

<sup>3</sup> [https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy\\_and\\_data\\_security\\_update\\_2016\\_web.pdf](https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf)



*Check: Reducing Risks to your Computer Systems*,<sup>4</sup> which provided early guidance to businesses about security information planning and risk analysis. Together, the Commission's numerous workshops, guidance documents, staff and Commission reports involve industry and other stakeholders in developing best practices and norms, and help frame and articulate the Agency's priorities.

Peer-to-Peer technology has been a focus of the FTC's privacy and security activities. As in other areas, the FTC provided opportunities for stakeholders to discuss the benefits and risks of P2P technology in the personal and business context. A workshop and staff report examined the risks to personal information created by P2P software. FTC Workshop on Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues December 15-16, 2004; Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, FTC Staff Report (2005)<sup>5</sup> at 8 (discussing academic research revealing inadvertent sharing of sensitive personal information and files; Nathaniel S. Good and Aaron Krekelberg, "Usability and Privacy: A Study of KaZaA P2P File-Sharing" (June 2002)). As in other areas, subsequent to its detailed fact finding and public consultation, the FTC released a business guide educating businesses about the risks Peer-to-Peer (P2P) file sharing software posed to personal

---

<sup>4</sup> <https://www.ftc.gov/system/files/documents/plain-language/bus58-security-check-reducing-risks-your-computer-systems.pdf>

<sup>5</sup> <https://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf>

information stored on systems. FTC, Peer-to-Peer File Sharing: A Guide to Business January 2010.<sup>6</sup> In addition to outlining risks, the Guide suggested methods for: identifying and removing P2P software that may have been installed by employees; mitigating risks if there was a business need for allowing P2P software on corporate networks; and, limiting the installation of P2P software. Among the risks discussed were the inadvertent file sharing at issue in this case; among the mitigations recommended were administrative security controls and commercial software to block access to sites used to download P2P software, and the adoption of administrative security controls to prevent employees from installing unapproved programs. *Id.* at 5-11.

The FTC's approach has provided a forum to ensure businesses and consumers are aware of the risks to personal data as technologies change, and business models evolve. Through the use of its convening, research, and guidance powers, the FTC has worked with experts in the field of data privacy and security to identify emerging risks and provide concrete guidance to businesses and consumers about how to mitigate them.

---

<sup>6</sup> <https://www.ftc.gov/system/files/documents/plain-language/bus46-peer-peer-file-sharing-guide-business.pdf>

**B. The FTC's Strategic Use of its Unfairness Authority Encourages and Supports Consumer Privacy Protection**

In this context, the FTC's strategic use of its unfairness authority in the data privacy context encourages corporations to develop "more forward-thinking and dynamic approaches to privacy policies, guided by a consumer-protection metric." Bamberger & Mulligan, Privacy on the Books, at 274. Bamberger and Mulligan's empirical inquiry found the threat of enforcement was "critical to the shaping of consumer-protection, rather than compliance-oriented, approaches to privacy." *Id.* In total, the FTC's approach ensures companies have ample opportunity for collective learning about best practices from their peers and experts in the field, and remain vigilant and proactive in using those insights to protect consumers' data.

Professors Bamberger and Mulligan's empirical research into leading chief privacy officers' practical experiences sheds light on the ways in which the FTC is driving progress in corporate information security practices through use of its unfairness enforcement authority. Seeking insight into how corporations define and protect consumer privacy in the course of their business, and in the shadow of FTC enforcement, the scholars conducted interviews with a select group of "chief privacy officers (CPOs) identified as industry leaders by their peers, government officials, and journalists." *Id.* at 251 (footnote omitted). The participating CPOs work within firms that are diverse "on every metric except size" and "hail both

from industries governed by sector-specific privacy statutes and from unregulated sectors.” *Id.* at 264. “Many focus on technology-intensive products and services, while others engage in more traditional lines of business.” *Id.* Some of the leading privacy officers interviewed are lawyers, “others have operational or technical expertise,” and “[s]ome work under the auspices of the corporate legal department” while “others work as free-standing officers.” *Id.*

The CPOs “uniformly pointed to the FTC’s role . . . in promoting the consumer protection understanding of privacy”—referencing the FTC’s long use of its authority to prevent unfair or deceptive acts or practices under Section 5 of the FTC Act “to take an active role in the governance of privacy protection, ranging from issuing guidance regarding appropriate practices for protecting personal consumer information, to bringing enforcement actions challenging information practices alleged to cause consumer injury.” *Id.* at 273.

As privacy officers focus on consumer protection—working within their firms to prevent “substantive harms” to clients such as “data breaches,” *id.* at 252—the interviewed CPOs identified “the FTC’s entrepreneurial use of its enforcement power” as an incentive to consider how the FTC’s flexible “consumer protection mandate might be applied to new practices, technologies, and contexts.” *Id.* at 310. “Several respondents stressed” that “a key to the effectiveness of FTC enforcement authority is the Commission’s ability to respond to harmful outcomes

by enforcing evolving standards of privacy protection as the market, technology, and consumer expectations change.” *Id.* at 273–74.

By contrast, in the CPOs’ experience, “specific procedural rules lack relevance to many privacy-impacting decisions that must be made by corporate managers.” *Id.* at 266. The privacy leaders specifically “described the failure of such rules to offer a touchstone for guiding privacy decision making in new contexts, as new types of products, technologies, and business models evolve.” *Id.*

One respondent “in a firm subject to FTC oversight explained the ways in which [an] enforcement action against that company transformed the understanding of privacy in their firm and others, from one centered on compliance with ex ante rules to one animated by the avoidance of consumer harm.” *Id.* at 274. Other respondents pointed to “previous FTC actions . . . as instigators for their firms’ decision to hire a privacy officer, or create or expand a privacy leadership function.” *Id.* Respondents described how the evolving privacy environment—including the FTC’s de facto requirement that firms implement “reasonable” data security measures—“fostered firms’ reliance on [CPOs’] professional judgment and the concomitant autonomy and power such dependence affords them within their organizations.” Kenneth A. Bamberger & Deirdre K. Mulligan, New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry, 33

Law & Pol’y 477, 479 (2011) [“An Initial Inquiry”]; *see also* Bamberger & Mulligan, Privacy on the Books, at 274 (describing how FTC enforcement actions motivated firms to focus and invest resources to protect personal data).

Leading CPOs report “the FTC’s roving enforcement authority,” Bamberger & Mulligan, Privacy on the Books, at 310, motivates firms to hire and empower privacy professionals and devote corporate resources to protecting consumer privacy in a holistic rather than bare-bones fashion. “In this sense, their accounts resonate with predictions from research on accountability in decisionmaking.” *Id.*

**C. Scholarship on Regulatory Governance Supports the FTC’s Broad Discretion with Respect to Unfairness Enforcement in the Data Privacy Sphere**

The interviewed CPOs’ experiences discussed above bear out what scholars of “new governance” methods have suggested—approaches that incorporate both agency flexibility and harness state and market forces can “spur and enlist the judgment and expertise of those inside firms to organize themselves in ways that best pursue the integration of public goals into corporate decision making” and “do so in a way that eschews one-time fixes in favor of dynamic and experimentalist problem solving.” Bamberger & Mulligan, An Initial Inquiry, at 487–88; *see also* Bamberger & Mulligan, Privacy on the Books, at 308.

Scholars have noted a “shift from traditional forms of static, rule-bound, top-down, ‘command-and-control’ regulation, to new forms of governance that

promote regulatory [flexibility], diversity, and revisability; that involve policy dynamism informed by experience and experimentation; that rely on transparency and create legal and market pressures for compliance; and that enlist stakeholders—including advocates, professionals, and regulated firms themselves—in achieving policy solutions.” Bamberger & Mulligan, An Initial Inquiry, 477–78. This shift is driven, partly, by the understanding that “specific rules often cannot reflect the large number of variables involved in achieving multifaceted regulatory goals,” *id.* at 480, and “uniform, static, approaches to regulation are particularly inapt to contexts characterized by rapid changes in technology and market infrastructure,” *id.* at 480. Moreover “a growing body of empirical and analytical research in the literature on regulation” demonstrates that “when regulators attempt to reflect the breadth of uncertain contextual factors in a regime of precise provisions, the proliferation of rules itself creates an unwieldy, confusing body of mandates and exceptions leading to uncertain and inconsistent application.” Kenneth A. Bamberger, Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State, 56 Duke L.J. 377, 387–88 (2006) (Regulation as Delegation”).

In other areas, regulators have sought to leverage industry expertise in security while protecting consumers. For example, HIPAA “engages private expertise by requiring individual regulated entities to determine, on a continuing

basis, what are the most salient threats facing their organizations. Efficacy is increased by shifting the cost of such decisions from regulators to individual entities and by allowing individual entities to use their expertise to make such decisions, but subjecting them to regulatory penalty for deficiencies in so doing. This approach increases legitimacy by allowing organizations a degree of input into their methods of compliance, thus increasing their input into the regulatory compliance process.” David Thaw, Enlightened Regulatory Capture, 89 Wash. L. Rev. 329, 362-363 (2014). This approach allows regulators to “harness private expertise not at the expense of the public interest, but rather in support of it.” *Id.* at 335.

Turning to the data privacy context, scholars note that “[r]isk, in particular, arises from the interplay of a variety of factors and manifests itself differently in heterogeneous firms. Its regulation, therefore, often cannot be boiled down to uniform rules governing behavior or mandating particular measurable outcomes.” Bamberger, Regulation as Delegation at 380. This has led regulators, like the FTC, to delegate “to regulated parties greater discretion in fulfilling legal goals.” Bamberger & Mulligan, Privacy on the Books, 295–96. This approach, grounded in new governance methods, “provides a means for enlisting the judgment of firm decisionmakers, drawing on their superior knowledge both about the ways risks manifest themselves in individual firm behaviors and business lines and about



available risk-management capacities and processes.” *Id.* at 305. In so doing, the FTC is “creat[ing] incentives” for private industry “to act in ways that enhance rather than weaken system security.” Deirdre K. Mulligan & Fred B. Schneider, Doctrine for Cybersecurity, Dædalus, Fall 2011, at 1. The Commission’s use of its unfairness enforcement authority has “focused industry . . . on understanding and respecting evolving and context-dependent [privacy] norms as they seek to deploy new technologies, new information practices, and new business models.” Bamberger & Mulligan, An Initial Inquiry, at 485, and focused firms on risks to personal data posed by changes in business models and technology.

These findings demonstrate that the FTC’s approach, which draws on innovative regulatory and governance methods, plays a key role in leveraging private expertise to advance public cybersecurity goals. Combining its “threat of coercive authority” and “role in developing a cross-field understanding of privacy” the FTC produces changes in corporate privacy management yielding more meaningful protections. Bamberger & Mulligan, Privacy on the Books, at 313. Artificially limiting the FTC’s powers to enforcing bright line rules, as LabMD and some of its amici suggest, threatens to undo that progress and hinder further advances in best practices for information security.

The ex ante regulations of the type LabMD and its Amici suggest are at odds with this empirical research and with research and practice in computer and

information security. Anderson, Ross, and Tyler Moore. “The Economics of Information Security.” *Science* 314.5799 (2006): 610-613.

At best, ex ante regulations reflect contemporary beliefs about how to best achieve the desired result, and codifying those beliefs into a static rule restricts regulators from adapting to changing circumstances and emerging new threats, and depresses industry investments in identifying and mitigating them. Bamberger & Mulligan, Privacy on the Books, at 303. A rules-based approach is at odds with years of computer and information security research and practice concluding that the constant evolution of technology and associated security threats means security is a process—“[t]here is no silver bullet and no one fix to ensure both privacy and security. Rather, it takes continual education, awareness and the application of appropriate controls in accordance with statute, standards and policies.” JC Cannon, *Privacy in Technology: Standards and Practices for Engineers and Security and IT Professionals* 18 (International Association of Privacy Professionals 2014). The FTC’s use of its unfairness authority to enforce data security standards on behalf of consumers, against a host of public processes that document risks and mitigations, creates incentives for companies to invest in processes that appropriately protect consumers’ personal information.

**II. THE TYPES OF INJURY AT ISSUE IN THIS AND OTHER DATA SECURITY CASES FALL SQUARELY WITHIN THE PREVENTATIVE ENFORCEMENT POWER THAT CONGRESS GRANTED THE FTC WITH RESPECT TO ACTS OR PRACTICES LIKELY TO CAUSE SUBSTANTIAL INJURY TO CONSUMERS**

The FTC's finding of injury and substantial risk of injury stemming from LabMD's disclosure of patient medical records here is consistent with prior health-related enforcement actions in which the FTC used its Section 5 authority to curb or prevent disclosure of consumers' confidential medical information. For example, in 2002 the FTC brought an enforcement action against pharmaceutical company Eli Lilly based on the company's unintentional disclosure of email addresses of people who subscribed to a list about the company's antidepressant drug. *In re Eli Lilly & Co.*, 133 F.T.C. 763 (2002).

One aspect of the harms here and in other health-information cases has been referred to as "insecurity." "Insecurity, in short, is a problem caused by the way our information is handled and protected." Daniel J. Solove, A Taxonomy of Privacy, 154 U. Penn. L. Rev. 477, 515 (2006). It "is the injury of being placed in a weakened state, of being made more vulnerable to a range of future harms." *Id.* at 518. Specifically, "[t]he potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability. In this respect, secondary use resembles the harm created by insecurity. The harm is a dignitary one, emerging from denying

people control over the future use of their data, which can be used in ways that have significant effects on their lives.” *Id.* at 520. As Prof. Chris Hoofnagle puts it, “Victims of security breaches have to live with the idea that some unknown person with unknowable motivations has their personal information and may try to profit from it through fraud or extortion. Revelation of this information—even basic information about websites visited or products purchased—can also be deeply embarrassing. In the medical context, some people go untreated or treat themselves so as to avoid the possibility that, somehow, others will learn that they were once treated for a loathsome disease or have had mental health treatment. . . .” Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy 224 (2016) [“Federal Trade Commission Privacy Law”].

The instant case focuses on a medical lab that analyzed blood, tissue, and urine samples, with a focus on urology and cancer. The patients faced the problem that others may know their diagnoses and even that at one point they suspected that they suffered from a condition treated by a urologist.

Data breaches, and the resulting insecurity, also lead to the concrete harms that come from an increased risk of medical identity theft. The World Privacy Forum, which has provided multiple studies of topic, defines medical identity theft as “when someone uses a person’s name and sometimes other parts of their identity—such as insurance information—without the person’s knowledge or

consent to obtain medical services or goods.” World Privacy Forum, “Medical Identity Theft,” available at <https://www.worldprivacyforum.org/category/med-id-theft/>, last visited February 16, 2017. Data breaches, as here, directly facilitate medical identity fraud, by enabling the criminal to provide accurate identity information (*e.g.*, email and Social Security number) linked with accurate clinical records (*e.g.*, blood tests). The criminal’s access to records from a breach “frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim’s name.” *Id.* These mistakes can lead to harms including financial fraud (the victim of identity theft is dunned for the fraudster’s medical bills) and medical harm (the erroneous blood test leads to a transfusion of an incompatible blood type). Based on such harms, the World Privacy Forum has specifically documented medical identity theft risks that result from a data breach.<sup>7</sup> These harms, though the result of recent technology, are precisely the kinds that Congress empowered the FTC to prevent, whether fully materialized or not. The FTC Act speaks expressly of the FTC’s power (and obligation) to “prevent” unfair acts or practices, 15 U.S.C. § 45(a)(2), and further empowers the FTC to regulate unfair practices that cause or are “likely to cause substantial injury to consumers,” *id.* at § 45(n). Both provisions

---

<sup>7</sup> World Privacy Forum, Medical ID Theft a Threat for Anthem Breach Victims, Key Tips, Feb. 6, 2015, available at <https://www.worldprivacyforum.org/category/med-id-theft>.

demonstrate that the FTC is charged with addressing harms before they fully develop in order to best protect consumers. Indeed, FTC scholars and its historical, legislative origins recognize the great care Congress took to provide the FTC with intentionally flexible unfairness powers.

“The FTC’s attributes—its expertise, its ability to provide certainty, its ability to be flexible, its ability to act to prevent problems, and its role as a forum for compromise—were forged by Congress to fight problems of trust and monopoly.” Hoofnagle, *Federal Trade Commission Privacy Law*, at 30. As it turns out, these attributes “are [also] remarkably well suited . . . for resolving modern privacy tussles.” *Id.*

When Congress passed the Wheeler-Lea Amendments to the FTC Act—“significantly broaden[ing] the scope of FTC power by allowing the Agency to prevent ‘unfair or deceptive acts or practices’ in addition to ‘unfair methods of competition’”—Congress chose not to “define ‘unfair or deceptive acts or practices.’” *Id.* at 37–38 (footnote omitted). Instead, Congress delegated to the Commission the responsibility to address consumer protection recognizing “[t]he benefit of this open-ended mandate was great flexibility to address new problems.” *Id.* at 38.

The benefit of this broad, flexible enforcement power is apparent from the FTC’s long history of addressing emerging threats to consumers as industries and

technology progress. For example, the Commission “focused on print advertising” for “the first thirty years” of its existence, but “[w]ith the rise of radio advertising,” in the mid-1930s, the FTC “was able to pivot and investigate false claims on the airwaves, without having to await enactment of a new law.” *Id.* It pivoted in the late 1940s “with the spread of television into Americans’ households” and, recently, “[t]he flexible approach adopted in Section 5 [of the FTC Act] enabled the Agency to take up privacy in the 1990s without an internet privacy statute.” *Id.* This flexibility is a *feature* of the Commission. Congress affirmatively took a policy decision in both 1914 (with respect to monopolies and trusts) and in 1938 (for consumer protection, “because business practices and technology were constantly evolving, causing new problems that Congress could not quickly act to remedy.” *Id.* at 120. Consequently, Section 5 of the FTC Act “cannot be defined in terms of constants. More broadly, it is a recognition of an ever-evolving commercial dexterity and the personal impact of economic power as important dimensions of trade.” *Id.* (quoting Eugene R. Baker & Daniel J. Baum, Section 5 of the Federal Trade Commission Act: A Continuing Process of Redefinition, 7 Vill. L. Rev. 517 (1962)); *see also id.* at 141 (“The [FTC’s] power to prevent unfair and deceptive trade practices is a remarkably broad one, . . . forged in decades of cases concerning false advertising and marketing.”).

Petitioner and some supporting amici argued incorrectly that the FTC is allowed to remedy only completed, economic harms. Such an exclusively economic-based approach guts the FTC's preventative powers, contravening Congress's express intent. Harms that Americans experience, care about and seek protection against are invasions of privacy. Within the last few years, the FTC has addressed and prohibited monitoring and geophysical location tracking technology (*In the Matter of Designware LLC*, Decision and Order, FTC File No. 1123151, Docket No. C-4390, Apr. 11, 2013); security risks associated with unauthorized access to or use of surveillance camera (*In the Matter of TRENDnet, Inc.*, Decision and Order, FTC File No. 1223090, Docket No. C-4426, Jan, 16, 2014); viewing data collected from a Smart TV (*Federal Trade Commission v. Vizio, Inc.* 2:17-CV-00758 (D. N.J., Feb 6, 2017)); data and information associated with routers and IP cameras (*Federal Trade Commission v. D-Link Corp. et al*, 3:17-CV-00039, (N.D. Cal., Jan 5, 2017)); and data associated with smartphone and tablet computer use (*In the Matter of HTC America Inc.*, *FTC File No. 1223049, Docket No. C-4406, June 25, 2013*). The insecurity surrounding identity theft and manipulation is a modern harm of the information age. The FTC's broad discretion with respect to unfairness enforcement meaningfully keeps pace with and addresses the harms citizens confront today.



### **III. HIPAA DOES NOT PREEMPT THE FTC'S AUTHORITY**

Appellant's argument that HIPAA implicitly repealed the FTC's Section 5 authority is unsupported by the text of the law, and regulations promulgated thereunder, and inconsistent with subsequent Congressional and agency action which furthered empowered the FTC to address the security of health information and fostered collaboration on rules and enforcement between HHS and the FTC. Moreover, Appellant's argument is inconsistent with how the FTC has operated for nearly a century.

There is no indication of Congressional intent to repeal the FTC's Section 5 authority in HIPAA itself. In fact, the HI-TECH Act, which modified the HIPAA rules, implicitly recognized a shared authority between HHS and the FTC. Moreover, in passing HIPAA, Congress preserved State data protection laws, which are regularly stricter than HIPAA, clearly showing a lack of intention to occupy the field. Implied repeal of federal law requires more direct and explicit actions than what is present here. The FTC's Section 5 power has never been found to stop because of a new federal law with overlapping regulatory domain. Finding implicit preemption would produce chaos, throwing nearly a century of consumer protection law into question, and creating a confusing, contentious, and unworkable regulatory system with boundaries constantly in dispute.

**A. The Text and History of HIPAA Provide No Basis for Finding that the Statute Preempts Section 5 of the FTC Act**

HIPAA was enacted in 1996. In discussing the scope of the privacy and security provisions, statute's text makes no mention of preempting any statute. Pub. L. 104-191. Pursuant to the statute, HHS issued a proposed Privacy Rule in 1999. HHS received over 52,000 public comments, and issued a final Privacy Rule in 2000. Under President Bush, the Privacy Rule was amended (though unrelated to preemption), and entered into final effect in 2003. U.S. Department of Health and Human Services. HIPAA for Professionals. <https://www.hhs.gov/hipaa/for-professionals/index.html>.

The 2000 final Privacy Rule discussed HIPAA's relationship to federal laws and state laws. The discussion of these two topics in the Privacy Rule governs how those issues are handled under the HIPAA Security Rule—the latter states explicitly that the relevant discussion for the Security Rule is in the 2000 Privacy Rule. 68 Fed. Reg. 8334, 8355 (Feb. 20, 2003).

In the section on “relationship with other federal law,” HHS discussed at least ten federal laws with comments or HHS analysis of possible preemption, repeal, or other effects from HIPAA. 65 Fed. Reg. 82462, 82481-87 (Dec. 28, 2000). Based on public comments, and its own analysis, HHS concluded: “There should be few instances in which conflicts exist between a statute or regulation and

the rules below.” *Id.* at 82481. Significantly, HHS did not analyze the FTC Act, indicating no commenter raised the possibility that Section 5 was preempted.<sup>8</sup>

If anyone involved in the Privacy Rule had surmised that HIPAA would deprive the FTC of Section 5 authority over millions of covered entities, and a large portion of commercial activity in the nation, there would have been considerable contemporaneous discussion.

**B. Congress has Continually Expanded the Entities that Can Protect Health Privacy and Security**

When Congress passed the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH Act”) adding a data breach notification requirement to HIPAA, it did not restrict the FTC from enforcing against HIPAA-regulated entities. Pub. L. No. 111-5, §§ 13001–13424, 123 Stat. 115, 226–79 (codified in scattered sections of 42 U.S.C.). This omission is salient as many of the amendments increased HHS’s enforcement powers, penalties, and scope. 42

---

<sup>8</sup> The only mention of the FTC in the Privacy Rule related to the Gramm-Leach-Bliley Act (“GLBA”), which allocates agency responsibility very specifically, gives the FTC residual authority over “financial institutions,” as defined in the GLBA, where no other financial enforcement agency has jurisdiction. The discussion focuses on the scope of FTC authority under GLBA in relation to state insurance commissioners who regulate health insurance companies. Because the state insurance commissioners occupied the field for health insurance companies, the FTC “clearly stated that it will not enforce the GLB privacy provisions against persons engaged in providing insurance.” *Id.* at 82484. The limited and residual authority of the FTC under GLBA contrasts sharply with the sweeping scope of the FTC’s jurisdiction under Section 5 of the FTC Act.

U.S.C. § 17934(a), (c) (2010). HITECH expanded HIPAA enforcement to business associates—millions of organizations that are not healthcare providers—creating overlap with Section 5 and rather than foreclosing FTC activity, it authorized state attorneys general to enforce HIPAA too. *See* 42 U.S.C. § 1320d-5(d) (2010); *Health Information Privacy: State Attorneys General*, U.S. Dep’t Health & Hum. Servs., <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/> (last visited Oct. 7, 2015).

### **C. The History of the FTC Does Not Support Preemption**

In the early days of FTC data protection enforcement, the possibility of overlapping jurisdiction was diminished because there were fewer laws regulating data protection issues. New data protection laws and regulation emerged after the FTC began policing privacy and security under its Section 5 authority in the mid-1990s.

Several laws gave the FTC specific and improved rulemaking authority and ability to directly assess fines and penalties, Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6505 (2012). CAN SPAM Act of 2003. Pub. L. 108-187; 15 U.S.C. § 7711; Gramm-Leach-Bliley Act (“GLBA”) §§ 504, 505, 522, 113 Stat. at 1439–41, 1447–48. These laws gave the FTC powers that augmented and extended its authority to address such issues under Section 5, and provided improved rulemaking authority in these specific contexts. Had Congress

thought the FTC was overreaching in its early Section 5 enforcement, the passage of these statutes would have been a logical time to reign in their actions. Instead, Congress did the opposite, and the result of these laws was to give the FTC a greater foothold in the data protection field.

Congress has never passed a data protection law restricting or prohibiting the use of Section 5. Given the breadth of Section 5 and its applicability to nearly every industry, plus the rise of new privacy legislation, combined with the embrace of data by almost every kind of business in the country, overlap has naturally increased.

Against this legal history, there is simply no textual or historical support for the categorical exclusion of data security, or for *any* single class of actions, absent hard evidence of Congressional intent to prohibit it.

The FTC was created to have intentionally general and expansive jurisdiction.<sup>9</sup> Instead of listing every area that the FTC's jurisdiction covers, the FTC Act specifically lists those it does not cover.<sup>10</sup> Congress did not amend that list when it passed HIPAA or any subsequent data protection laws.<sup>11</sup>

Section 5's inevitable overlap with other statutes and regulatory domains is necessary and manageable. The FTC routinely shares regulatory authority with

---

<sup>9</sup> See *supra* Part I.B.1.

<sup>10</sup> 15 U.S.C. §§ 13c, 45(a)(2) (2012). Non-profit entities are ostensibly not engaged in "commerce."

<sup>11</sup> *Id.* (citing 15 U.S.C. § 45(a)(2)).

other administrative agencies. Consumer protection is involved in numerous other domains because the range of commerce is so vast. Many statutes and administrative agencies inevitably overlap with the FTC's potential reach, yet courts have explicitly found this overlap not to curtail the FTC's jurisdiction.<sup>12</sup> For example, the FTC has worked with the FDA for decades regarding certain food and drugs advertising.<sup>13</sup> Additionally, in examining FTC's deceptive advertising overlap with the Commodities Exchange Act and Investment Advisors Act ("IAA"), one court stated, "[t]he proscriptions of the IAA are not diminished or confused merely because investment advisers must also avoid that which the FTC Act proscribes. And, because these statutes are 'capable of co-existence,' it becomes the *duty* of this court 'to regard each as effective'—at least absent clear congressional intent to the contrary."<sup>14</sup>

The FTC and HHS often coordinate enforcement actions for violations implicating HIPAA and the FTC Act.<sup>15</sup> The data security standards the FTC has

---

<sup>12</sup> See, e.g., *FTC v. Ken Roberts Co.*, 276 F.3d 583, 593 (D.D.C. 2001).

<sup>13</sup> See Memorandum of Understanding Between the Federal Trade Commission and the Food and Drug Administration, 36 Fed. Reg. 18,539, 18,539 (Sept. 16, 1971); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1986) (finding no evidence to support constrain FTC jurisdiction).

<sup>14</sup> *Ken Roberts Co.*, 276 F.3d at 593 (quoting *Morton v. Mancari*, 417 U.S. 535, 551 (1974)).

<sup>15</sup> See Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164).

developed are consistent with those in the HIPAA Security Rule. Regulatory overlap has not resulted in significant inconsistencies or confusion.


The FTC's data protection authority overlapping with HIPAA is not a unique case, but one example among many of overlap that understandably arise given the breadth of the FTC's Section 5 authority. Moreover, without a federal omnibus data protection statute, the basic U.S. approach to data protection is a series of different laws regulating different corners of the economy. A rigid prohibition on regulatory overlap would prove quite challenging and chaotic. Agencies would clash in carving out contiguous borders when their regulatory scopes overlap. And these borders would need adjusting with each new law that creates potential overlap. In sum, the idea that potential regulatory overlap disqualifies the FTC from regulating data security is not supported by the law, history, or practice.

### **CONCLUSION**

For the foregoing reasons, LabMD's petition should be denied.

Respectfully submitted,

Michael W. Sobol  
Lief Cabraser Heimann &  
Bernstein, LLP  
275 Battery Street, 29th Floor  
San Francisco, CA 94111-3339  
415.956.1000  
msobol@lchb.com

  
\_\_\_\_\_  
Nicholas R. Diamand  
Lief Cabraser Heimann &  
Bernstein, LLP  
250 Hudson Street, 8th Floor  
New York, NY 10013-1413  
212.355.9500  
ndiamand@lchb.com

Laura B. Heiman  
Lieff Cabraser Heimann &  
Bernstein, LLP  
One Nashville Place  
150 Fourth Avenue, North, Suite 1650  
Nashville, TN 37219-2423  
615.313.9000  
lheiman@lchb.com



**CERTIFICATE OF COMPLIANCE**

The undersigned counsel hereby certifies that this brief complies with Fed. R. App. P. 32(a) because, excluding the parts exempted by Fed. R. App. P. 32(f) and 11th Cir. R. 32-4, this brief contains 6,357 words and has been prepared in a 14-point proportionally spaced typeface.

Dated: February 16, 2017

Respectfully submitted,

/s/ Laura B. Heiman

Laura B. Heiman  
Lief Cabraser Heimann &  
Bernstein, LLP  
One Nashville Place  
150 Fourth Avenue, North, Suite 1650  
Nashville, TN 37219-2423  
615.313.9000  
lheiman@lchb.com

**CERTIFICATE OF SERVICE**

I hereby certify that, on February 16, 2017, I filed the foregoing document in the United States Court of Appeals for the Eleventh Circuit using the Court's Electronic Case Files (ECF) system, which generates a notice that is emailed to attorneys of record registered to use the ECF System.

Dated: February 16, 2017

Respectfully submitted,

/s/ Laura B. Heiman

Laura B. Heiman  
Lieff Cabraser Heimann &  
Bernstein, LLP  
One Nashville Place  
150 Fourth Avenue, North, Suite 1650  
Nashville, TN 37219-2423  
615.313.9000  
lheiman@lchb.com

**ADDENDUM: IDENTITY OF AMICI CURIAE**

**Kenneth A. Bamberger** is the Rosalinde and Arthur Gilbert Foundation Professor of Law at the University of California, Berkeley, and a Faculty Director of the Berkeley Center for Law and Technology. He is the co-author of *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (MIT Press) the first empirical, comparative, international exploration of how legal choices in the U.S. and four European countries impact corporate privacy practice, and has published widely on administrative law, administrative agencies, and the regulation of privacy and technology.

**Woodrow Hartzog** is the Starnes Professor of Law at Samford University's Cumberland School of Law and an Affiliate Scholar at Stanford Law School's Center for Internet and Society. He has written over 30 academic works on privacy, law, and technology, including multiple articles about the FTC.

**Chris Jay Hoofnagle** is Adjunct Full Professor of Information and of Law at the University of California, Berkeley. He is the author of *Federal Trade Commission Privacy Law and Policy* (Cambridge University Press 2016).

**William McGeveran** is Associate Professor of Law and Solly Robins Distinguished Research Fellow at the University of Minnesota Law School. He has written a casebook about privacy law and multiple journal articles in the field, including research about FTC enforcement.

**Deirdre K. Mulligan** is an Associate Professor in the School of Information at UC Berkeley, and a faculty Director of the Berkeley Center for Law & Technology and UC Berkeley School of Law. Mulligan is the co-author of *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (MIT Press) the first empirical, comparative, international exploration of how legal choices in the U.S. and four European countries impact corporate privacy practice, and more than 50 articles on privacy and security law, and technology.

**Paul Ohm** is a Professor of Law at the Georgetown University Law Center. His work focuses on information privacy, computer crime law, and technology and law.

**Daniel J. Solove** is the John Marshall Harlan Research Professor of Law at George Washington University Law School. He is the author of 10 books and more than 50 articles about privacy and security law, including several casebooks as well as many works about the FTC.

**Peter Swire** is the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business. He is the author of six books and over 50 articles about privacy and security law. From 1999 to 2001, he served as Chief Counselor for Privacy in the U.S. Office of Management and Budget, where he was White House coordinator for the 1999 proposed and 2000 final HIPAA Privacy Rule.