

# **EXHIBIT**

**1**

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Edith Ramirez, Chairwoman  
Julie Brill  
Maureen K. Ohlhausen  
Joshua D. Wright

\_\_\_\_\_  
In the Matter of )  
)  
)

LabMD, Inc., )  
a corporation. )  
)  
)  
)  
\_\_\_\_\_)

DOCKET NO. 9357

PROVISIONALLY REDACTED  
PUBLIC VERSION

COMPLAINT

The Federal Trade Commission (“Commission”), having reason to believe that LabMD, Inc. (“LabMD” or “respondent”), a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

RESPONDENT’S BUSINESS

1. Respondent LabMD is a Georgia corporation with its principal office or place of business at 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339.
2. The acts and practices of respondent alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.
3. Since at least 2001, respondent has been in the business of conducting clinical laboratory tests on specimen samples from consumers and reporting test results to consumers’ health care providers.
4. Respondent files insurance claims for charges related to the clinical laboratory tests with health insurance companies. Insured consumers typically pay the part of respondent’s charges not covered by insurance; uninsured consumers are responsible for the full amount of the charges. Consumers in many instances pay respondent’s charges with credit cards or personal checks.

5. Respondent tests samples from consumers located throughout the United States.
6. In performing tests, respondent routinely obtains information about consumers, including, but not limited to: names; addresses; dates of birth; gender; telephone numbers; Social Security numbers (“SSN”); medical record numbers; bank account or credit card information; health care provider names, addresses, and telephone numbers; laboratory tests, test codes and results, and diagnoses; clinical histories; and health insurance company names and policy numbers (collectively, “personal information”).
7. Respondent has accumulated and maintains personal information for nearly one million consumers.
8. Respondent operates computer networks in conducting its business. The computer networks include computers, servers, and other devices in respondent’s corporate offices and laboratory, computers used by its personnel in different parts of the country, and computers that respondent provides to some health care providers.
9. Among other things, respondent uses the computer networks to: receive orders for tests from health care providers; report test results to health care providers; file insurance claims with health insurance companies; prepare bills and other correspondence to consumers; obtain approvals for payments made by consumers with credit cards; and prepare medical records. For example, respondent’s billing department uses the computer networks to generate or access documents related to processing claims and payments, such as:
  - (a) monthly spreadsheets of insurance claims and payments (“insurance aging reports”), which may include personal information such as consumer names, dates of birth, SSNs, the American Medical Association current procedural terminology (“CPT”) codes for the laboratory test conducted, and health insurance company names, addresses, and policy numbers;
  - (b) spreadsheets of payments received from consumers (“Day Sheets”), which may include personal information such as consumer names, SSNs, and methods, amounts, and dates of payments; and
  - (c) copies of consumer checks, which may include personal information such as names, addresses, telephone numbers, payment amounts, bank names and routing numbers, and bank account numbers (“copied checks”).

## RESPONDENT'S SECURITY PRACTICES

10. At all relevant times, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. Among other things, respondent:
  - (a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information. Thus, for example, employees were allowed to send emails with such information to their personal email accounts without using readily available measures to protect the information from unauthorized disclosure;
  - (b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. By not using measures such as penetration tests, for example, respondent could not adequately assess the extent of the risks and vulnerabilities of its networks;
  - (c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
  - (d) did not adequately train employees to safeguard personal information;
  - (e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication;
  - (f) did not maintain and update operating systems of computers and other devices on its networks. For example, on some computers respondent used operating systems that were unsupported by the vendor, making it unlikely that the systems would be updated to address newly discovered vulnerabilities; and
  - (g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks. For example, respondent did not use appropriate measures to prevent employees from installing on computers applications or materials that were not needed to perform their jobs or adequately maintain or review records of activity on its networks. As a result, respondent did not detect the installation or use of an unauthorized file sharing application on its networks.
11. Respondent could have corrected its security failures at relatively low cost using readily available security measures.

12. Consumers have no way of independently knowing about respondent's security failures and could not reasonably avoid possible harms from such failures, including identity theft, medical identity theft, and other harms, such as disclosure of sensitive, private medical information.

### **PEER-TO-PEER FILE SHARING APPLICATIONS**

13. Peer-to-peer ("P2P") file sharing applications are often used to share music, videos, pictures, and other materials between persons and entities using computers with the same or a compatible P2P application ("P2P network").
14. P2P applications allow a user to both designate files on the user's computer that are available to others on a P2P network and search for and access designated files on other computers on the P2P network.
15. After a designated file is shared with another computer, it can be passed along among other P2P network users without being downloaded again from the original source. Generally, once shared, a file cannot with certainty be removed permanently from a P2P network.
16. Since at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks.

### **SECURITY INCIDENTS**

17. In May 2008, a third party informed respondent that its June 2007 insurance aging report (the "P2P insurance aging file") was available on a P2P network through Limewire, a P2P file sharing application.
18. After receiving the May 2008 notice that the P2P insurance aging file was available through Limewire, respondent determined that:
  - (a) Limewire had been downloaded and installed on a computer used by respondent's billing department manager (the "billing computer");
  - (b) at that point in time, the P2P insurance aging file was one of hundreds of files that were designated for sharing from the billing computer using Limewire; and
  - (c) Limewire had been installed on the billing computer no later than 2006.
19. The P2P insurance aging file contains personal information about approximately 9,300 consumers, including names, dates of birth, SSNs, CPT codes, and, in many instances, health insurance company names, addresses, and policy numbers.

20. Respondent had no business need for Limewire and removed it from the billing computer in May 2008, after receiving notice.
21. In October 2012, the Sacramento, California Police Department found more than 35 Day Sheets and a small number of copied checks in the possession of individuals who pleaded no contest to state charges of identity theft. These Day Sheets include personal information, such as names and SSNs, of several hundred consumers in different states. Many of these consumers were not included in the P2P insurance aging file, and some of the information post-dates the P2P insurance aging file. A number of the SSNs in the Day Sheets are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identity thieves.

### **VIOLATION OF THE FTC ACT**

22. As set forth in Paragraphs 6 through 21, respondent's failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information, including dates of birth, SSNs, medical test codes, and health information, caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.
23. The acts and practices of respondent as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a).

### **NOTICE**

Notice is hereby given to the respondent that the twenty-eighth day of April, 2014, at 10:00 a.m., is hereby fixed as the time, and the Federal Trade Commission offices at 600 Pennsylvania Avenue, N.W., Room 532-H, Washington, D.C. 20580, as the place when and where a hearing will be had before an Administrative Law Judge of the Federal Trade Commission, on the charges set forth in this complaint, at which time and place you will have the right under the Federal Trade Commission Act to appear and show cause why an order should not be entered requiring you to cease and desist from the violations of law charged in this complaint.

You are notified that the opportunity is afforded you to file with the Federal Trade Commission an answer to this complaint on or before the fourteenth (14th) day after service of it upon you. An answer in which the allegations of the complaint are contested shall contain a concise statement of the facts constituting each ground of defense; and specific admission, denial, or explanation of each fact alleged in the complaint or, if you are without knowledge thereof, a statement to that effect. Allegations of the complaint not thus answered shall be deemed to have been admitted.

If you elect not to contest the allegations of fact set forth in the complaint, the answer shall consist of a statement that you admit all of the material facts to be true. Such an answer shall constitute a waiver of hearings as to the facts alleged in the complaint and, together with the complaint, will provide a record basis on which the Commission shall issue a final decision containing appropriate findings and conclusions, and a final order disposing of the proceeding. In such answer, you may, however, reserve the right to submit proposed findings of fact and conclusions of law under Rule 3.46 of the Commission's Rules of Practice for Adjudicative Proceedings.

Failure to answer within the time above provided shall be deemed to constitute a waiver of your right to appear and to contest the allegations of the complaint, and shall authorize the Commission, without further notice to you, to find the facts to be as alleged in the complaint and to enter a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding.

The Administrative Law Judge shall hold a prehearing scheduling conference not later than ten (10) days after the answer is filed by the respondent. Unless otherwise directed by the Administrative Law Judge, the scheduling conference and further proceedings will take place at the Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Room 532-H, Washington, D.C. 20580. Rule 3.21(a) requires a meeting of the parties' counsel as early as practicable before the prehearing scheduling conference, but in any event no later than five (5) days after the answer is filed by the respondent. Rule 3.31(b) obligates counsel for each party, within five (5) days of receiving respondent's answer, to make certain disclosures without awaiting a formal discovery request.

The following is the form of order which the Commission has reason to believe should issue if the facts are found to be as alleged in the complaint. If, however, the Commission should conclude from record facts developed in any adjudicative proceedings in this matter that the proposed order provisions might be inadequate to fully protect the consuming public, the Commission may order such other relief as it finds necessary or appropriate.

Moreover, the Commission has reason to believe that, if the facts are found as alleged in the complaint, it may be necessary and appropriate for the Commission to seek relief to redress injury to consumers, or other persons, partnerships or corporations, in the form of restitution for past, present, and future consumers and such other types of relief as are set forth in Section 19(b) of the Federal Trade Commission Act. The Commission will determine whether to apply to a court for such relief on the basis of the adjudicative proceedings in this matter and such other factors as are relevant to consider the necessity and appropriateness of such action.

## ORDER

### DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
2. Unless otherwise specified, “respondent” shall mean LabMD, Inc., and its successors and assigns.
3. “Affected Individual” shall mean any consumer whose personal information LabMD has reason to believe was, or could have been, accessible to unauthorized persons before the date of service of this order, including, but not limited to, consumers listed in the Insurance File and the Sacramento Documents.
4. “Insurance File” shall mean the file containing personal information about approximately 9,300 consumers, including names, dates of birth, Social Security numbers, health insurance company names and policy numbers, and medical test codes, that was available to a peer-to-peer file sharing network through a peer-to-peer file sharing application installed on a computer on respondent’s computer network.
5. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a “cookie” or processor serial number.
6. “Sacramento Documents” shall mean the documents identified in Appendix A.

#### I.

**IT IS ORDERED** that the respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program;
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by Subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

## II.

**IT IS FURTHER ORDERED** that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part I of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No.1023099. Provided, however, that in lieu of overnight courier, assessments may be sent by first-class mail, but only if an electronic version of any such assessment is contemporaneously sent to the Commission at [Debrief@ftc.gov](mailto:Debrief@ftc.gov).

### III.

**IT IS FURTHER ORDERED** that respondent shall provide notice to Affected Individuals and their health insurance companies within 60 days of service of this order unless an appropriate notice has already been provided, as follows:

- A. Respondent shall send the notice to each Affected Individual by first class mail, only after obtaining acknowledgment from the Commission or its staff that the form and substance of the notice satisfies the provisions of the order. The notice must be easy to understand and must include:
  - 1. a brief description of why the notice is being sent, including the approximate time period of the unauthorized disclosure, the types of personal information that were or may have been disclosed without authorization (*e.g.*, insurance information, Social Security numbers, etc.),

and the steps respondent has taken to investigate the unauthorized disclosure and protect against future unauthorized disclosures;

2. advice on how Affected Individuals can protect themselves from identity theft or related harms. Respondent may refer Affected Individuals to the Commission's identity theft website ([www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)), advise them to contact their health care providers or insurance companies if bills don't arrive on time or contain irregularities, or to obtain a free copy of their credit report from [www.annualcreditreport.com](http://www.annualcreditreport.com) and monitor it and their accounts for suspicious activity, or take such other steps as respondent deems appropriate; and
  3. methods by which Affected Individuals can contact respondent for more information, including a toll-free number for 90 days after notice to Affected Individuals, an email address, a website, and mailing address.
- B. Respondent shall send a copy of the notice to each Affected Individual's health insurance company by first class mail.
- C. If respondent does not have an Affected Individual's mailing address in its possession, it shall make reasonable efforts to find such mailing address, such as by reviewing online directories, and once found, shall provide the notice described in Subpart A, above.

#### IV.

**IT IS FURTHER ORDERED** that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

- A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, notice letters required by Part III of this order and documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

## V.

**IT IS FURTHER ORDERED** that respondent shall deliver a copy of this order to: (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order; and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.

## VI.

**IT IS FURTHER ORDERED** that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at [Debrief@ftc.gov](mailto:Debrief@ftc.gov).

## VII.

**IT IS FURTHER ORDERED** that respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, they shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission in writing, all notices required by this Part shall be emailed to [Debrief@ftc.gov](mailto:Debrief@ftc.gov) or sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099.

## VIII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. any Part in this order that terminates in less than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that each respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

**IN WITNESS WHEREOF**, the Federal Trade Commission has caused this complaint to be signed by its Secretary and its official seal to be hereto affixed, at Washington, D.C. this twenty-eighth day of August, 2013.

By the Commission.

Donald S. Clark  
Secretary

# **EXHIBIT**

**10**

**Forum Europe Fourth Annual EU Data Protection and Privacy Conference**  
**Commissioner Julie Brill's Keynote Address**  
**September 17, 2013**  
**Brussels, Belgium**

Good morning. I would like to thank Forum Europe for the invitation to participate in this important conference today. I am always delighted to have the opportunity to engage with my EU counterparts on issues that are important to all of us, and I see many of my friends in the audience today.

A lot has changed since this past April when I was last in Brussels. The revelations about the U.S. National Security Agency's programs<sup>1</sup> have sparked a global debate about government surveillance and its effect on individual privacy. As many of you know, I have spent a lifetime working on consumer protection and privacy issues, so it should be no surprise that this is a debate I welcome. It is a conversation that is long overdue, but I also think it is important that we have the right conversation—one that is open and honest, practical and productive. As we move forward with this conversation, my personal view is that there are some important facts that we should keep in mind as we collectively attempt to answer some very tough questions:

- First, whether we call privacy a “fundamental right” or a Constitutional right, the U.S., EU, and many other countries around the world place tremendous value on privacy. Our legislative and regulatory frameworks may differ, but the acknowledgment of the need for privacy protections and the principles underlying how we define those protections are, at their core, the same.<sup>2</sup>
- Second, national security exceptions in laws, including privacy laws, are the norm, not the exception, for countries around the globe, including EU Member States and third countries that have received European Commission adequacy determinations.<sup>3</sup> As we revisit the proper scope of government surveillance, the

---

<sup>1</sup> See Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (Jun. 9, 2013), available at <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

<sup>2</sup> See Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Mentor Group Forum for EU-US Legal Economic Affairs: Remarks to the Mentor Group (Apr. 16, 2013), available at <http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf>.

<sup>3</sup> See, e.g., Directive 1995/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2005 O.J. (L 281) 31, 42, available at [http://ec.europa.eu/justice/policies/privacy/docs/95-46-ec/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/95-46-ec/dir1995-46_part1_en.pdf) [hereinafter “EU Data Protection Directive”]; Personal Information Protection and Electronic Documents Act, R.S.C. 2000, c. 5, 6-8, 11, available at <http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf> (Can.). See generally Christopher Wolf, *An Analysis of Service Provider Transparency Reports on Government Requests for Data*, HOGAN LOVELLS (Aug. 27, 2013), <http://www.hldataprotection.com/files/2013/08/Hogan-Lovells-White-Paper-Analysis-of-Transparency-Reports.pdf>.

sufficiency of procedural safeguards, and how to “balance the ends with the means”,<sup>4</sup> we should examine these issues with a global lens, as these challenges are not unique to a single sovereign.

- Third, the recent events provide a teachable moment that should encourage us to redouble our efforts on improving transparency and privacy protections for consumers in the commercial sphere. We have a renewed opportunity to be proactive rather than reactive, and to move the separate but equally important conversation about enhancing consumer privacy forward, not backward. It is important to acknowledge that commercial privacy and national security issues are two distinctly separate issues. Indeed, the EU has recognized this distinction, as the data protection laws do not apply to national security issues.<sup>5</sup> And this is the right approach, helping to ensure the solutions we develop will be tailored to each set of problems we seek to address.

At the Federal Trade Commission, we address commercial privacy. We do not have criminal jurisdiction, or jurisdiction over national security issues. Of course, there are other U.S. officials who are charged with addressing those issues, and they are eager to do so.

The FTC has a long tradition of using its authority against unfair or deceptive practices to protect consumer privacy. We take action against companies that fail to comply with their own privacy policies or otherwise misrepresent their information management practices. And, just as importantly, we also address unfair collection and use of personal information that inflicts harm on consumers that they cannot reasonably avoid, and that does not offer offsetting benefits to consumers or competition.<sup>6</sup>

As specific privacy and data security issues have arisen over the past 40 years, Congress has supplemented the FTC’s broad remedial authority by charging us and other agencies with enforcing other privacy laws, including laws designed to protect financial<sup>7</sup> and health information,<sup>8</sup> children,<sup>9</sup> and information used for credit, insurance, employment and housing decisions.<sup>10</sup>

---

<sup>4</sup> *Full Transcript: President Obama’s Press Conference with Swedish Prime Minister Fredrik Reinfeldt in Stockholm*, WASH. POST, Sept. 4, 2013, available at [http://www.washingtonpost.com/politics/full-transcript-president-obamas-press-conference-with-swedish-prime-minister-fredrik-reinfeldt-in-stockholm/2013/09/04/35e3e08e-1569-11e3-804b-d3a1a3a18f2c\\_story.html](http://www.washingtonpost.com/politics/full-transcript-president-obamas-press-conference-with-swedish-prime-minister-fredrik-reinfeldt-in-stockholm/2013/09/04/35e3e08e-1569-11e3-804b-d3a1a3a18f2c_story.html).

<sup>5</sup> See EU Data Protection Directive, *supra* note 3, at 42.

<sup>6</sup> 15 U.S.C. § 45(n).

<sup>7</sup> Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.); Fair Credit Reporting Act of 1970 (FRCA), Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681u).

<sup>8</sup> Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. §§ 201 note, 300jj *et seq.*, 17901.

At the FTC, protecting consumer privacy is one of our most important missions. We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of companies that operate throughout the Internet and mobile ecosystem. Our most well-known cases – against Google,<sup>11</sup> Facebook,<sup>12</sup> and MySpace<sup>13</sup> – have led to orders that, for the next 20 years, govern the data collection and use activities of these companies. And in each of these cases we have addressed the companies’ failure to comply with the U.S.-EU Safe Harbor.

We have also brought myriad cases against companies that are not household names, but whose practices crossed the line. We’ve sued companies spamming consumers and installing spyware on their computers.<sup>14</sup> We’ve challenged companies that failed to properly secure consumer information.<sup>15</sup> We have sued ad networks,<sup>16</sup> analytics companies,<sup>17</sup> data brokers,<sup>18</sup> and software developers.<sup>19</sup> We have vigorously

---

<sup>9</sup> Children’s Online Privacy Protection Act of 1998 (COPPA), Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

<sup>10</sup> 15 U.S.C. §§ 1681-1681t.

<sup>11</sup> In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* <http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf> (decision and order).

<sup>12</sup> In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* <http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf> (decision and order).

<sup>13</sup> In the Matter of Myspace, LLC, FTC File No. 102 3058 (Aug. 30, 2012) *available at* <http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf> (decision and order).

<sup>14</sup> *See, e.g., FTC v. Flora*, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* <http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf>; *FTC v. CyberSpy Software, LLC, et al.*, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), *available at* <http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf> (stipulated final order).

<sup>15</sup> *See, e.g., In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), *available at* <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf> (administrative complaint).

<sup>16</sup> *See, e.g., In the Matter of Epic Marketplace, Inc. et al.*, FTC File No. 112 3182 (Mar. 13, 2013), *available at* <http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf> (decision and order).

<sup>17</sup> *See, e.g., In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Apr. 3, 2012), *available at* <http://www.ftc.gov/os/caselist/1023116/120403upromisedo.pdf> (decision and order).

<sup>18</sup> *See, e.g., U.S. v. Spokeo, Inc.*, No. 12-CV-05001 (C.D. Cal. June 19, 2012), *available at* <http://ftc.gov/os/caselist/1023163/120612spokeoorder.pdf> (consent decree and order); *In the Matter of Filiquarian Pub. LLC et al.*, FTC File No. 112 3195 (Apr. 30, 2013), *available at* <http://www.ftc.gov/os/caselist/1123195/130501filquariando.pdf> (decision and order).

<sup>19</sup> *See, e.g., In the Matter of DesignerWare LLC*, FTC File No. 112 3151 (Apr. 11, 2013), *available at* <http://www.ftc.gov/os/caselist/1123151/designerware/130415designerwaredo.pdf> (decision and order).

enforced the Children’s Online Privacy Protection Act.<sup>20</sup> And with the world moving to mobile, we have targeted app developers as well as handheld device manufacturers engaged in inappropriate data collection and use practices.<sup>21</sup>

As part of our ongoing effort to address privacy issues in the changing technological landscape, just two weeks ago we brought our first action involving the Internet of Things.<sup>22</sup> In that case, the company failed to secure the software for its Internet-accessible video cameras, which put hundreds of private lives on public display.<sup>23</sup>

Together, these enforcement efforts have established what some scholars call “the common law of privacy” in the United States, in which the FTC articulates – to industry, defense counsel, consumer groups and other stakeholders – in an incremental, but no less effective way, the privacy practices that are deceptive or unfair.<sup>24</sup>

In addition to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. We have held hearings and issued reports on cutting edge issues, including facial recognition technology<sup>25</sup>, kids apps,<sup>26</sup> mobile privacy disclosures,<sup>27</sup> and mobile

---

<sup>20</sup> See, e.g., *U.S. v. Path, Inc.*, No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (Consent decree and order), available at <http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf>.

<sup>21</sup> See, e.g., *In the Matter of HTC, Inc.*, FTC File No. 122 3049 (June 25, 2013), available at <http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf> (decision and order).

<sup>22</sup> *In the Matter of TRENDnet, Inc.*, FTC File No. 122 3090 (Sept. 4, 2013), available at <http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf> (agreement containing consent order); see also Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement*, N.Y. TIMES, Sept. 8, 2013, available at <http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things>.

<sup>23</sup> See *id.*

<sup>24</sup> Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (forthcoming 2014), available at <http://ssrn.com/abstract=2312913>. See also Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011), (discussing how chief privacy officers reported that “state-of-the-art privacy practices” need to reflect both established black letter law and FTC cases and best practices, including FTC enforcement actions and FTC guidance); Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States*, BNA Privacy and Security Law Report, Oct. 25, 2010, available at [http://www.justice.gov/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer\\_WOLFDataProtectionandPrivacyCommissioners.pdf](http://www.justice.gov/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf) (FTC consent decrees have “created a ‘common law of consent decrees,’ producing a set of data protection rules for businesses to follow”).

<sup>25</sup> See Press Release, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), available at <http://ftc.gov/opa/2012/10/facialrecognition.shtm>.

<sup>26</sup> See FED. TRADE COMM’N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012), available at <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf>.

payments.<sup>28</sup> Last year the FTC issued its landmark privacy report in which the agency developed a new framework for addressing privacy in the U.S., including best practices for companies to follow based on three core principles: privacy by design, simplified choice, and greater transparency around data collection and use.<sup>29</sup> We called on companies to operationalize the report's recommendations by developing better just-in-time notices and robust choice mechanisms, particularly for health and other sensitive information.<sup>30</sup>

The FTC is also actively studying the data broker industry to learn more about the ways that companies collect, buy, and sell consumer data. We hope to issue a report later this year on how data brokers could improve their privacy practices.<sup>31</sup> In last year's privacy report, the FTC called on Congress to enact data broker legislation that would increase the transparency of the practices of data brokers.<sup>32</sup>

But we don't have to wait for legislation. I recently launched "Reclaim Your Name", a comprehensive initiative to give consumers the means they need to reassert control over their personal data.<sup>33</sup> I call on industry to develop a user-friendly, one-stop online shop to provide consumers with some tools to find out about data broker practices and to exercise reasonable choices about them.<sup>34</sup> Acxiom, the largest data broker in the U.S., has taken the first step toward greater transparency by launching [aboutthedata.com](http://aboutthedata.com), a web portal that allows consumers to access, correct, and suppress the data that the company maintains about them.<sup>35</sup> And while there is certainly room for Acxiom to

---

<sup>27</sup> See Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), available at <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>.

<sup>28</sup> See FED. TRADE COMM'N, *Plastic, Paper, or Mobile? An FTC Workshop on Mobile Payments* (March 2013), available at <http://www.ftc.gov/os/2013/03/130306mobilereport.pdf>.

<sup>29</sup> See FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> [hereinafter "FTC Privacy Report"].

<sup>30</sup> See *id.*

<sup>31</sup> See Press Release, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 12, 2012), available at <http://www.ftc.gov/opa/2012/12/databrokers.shtm>.

<sup>32</sup> See FTC Privacy Report, *supra* note 29, at 14.

<sup>33</sup> See Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at 23<sup>rd</sup> Computers Freedom and Privacy Conference: Reclaim Your Name (June 26, 2013), available at <http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf>.

<sup>34</sup> See *id.* See also Julie Brill, Op-Ed., *Demanding Transparency from Data Brokers*, WASH. POST, Aug. 15, 2013, available at [http://articles.washingtonpost.com/2013-08-15/opinions/41412540\\_1\\_data-brokers-fair-credit-reporting-act-data-fuel](http://articles.washingtonpost.com/2013-08-15/opinions/41412540_1_data-brokers-fair-credit-reporting-act-data-fuel).

<sup>35</sup> See generally Natasha Singer, *Acxiom Lets Consumers See Data It Collects*, N.Y. TIMES, Sept. 4, 2013, available at <http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html?pagewanted=all>.

improve its portal, I encourage other industry players to join Acxiom and step up to the plate to provide consumers with greater transparency about their data collection and use practices.

The FTC has also supported baseline privacy legislation.<sup>36</sup> The Obama Administration has been actively working on privacy legislation that would implement its Consumer Privacy Bill of Rights.<sup>37</sup>

Through the FTC Act and other US privacy and data protection laws, the FTC's privacy report and other policy initiatives, and the Obama Administration's Consumer Privacy Bill of Rights, the US aims to achieve many of the same objectives that are outlined in the draft EU data protection regulation. For instance, on both sides of the Atlantic, we are striving to protect children's privacy; spur companies to implement privacy by design, increase transparency, and adopt accountability measures; and require companies to provide notice about data breaches. As the technological challenges facing the EU and the US have grown, so has our common ground in protecting consumers. In some instances, we differ on how to achieve these common goals. For example, we both believe that consumer consent is important, but we have different approaches as to when and how that consent should be obtained. The particular solutions we develop may differ, but the challenges we face and our desire to solve them are the same.

In a world with diverse privacy frameworks, interoperability is critical. We should work together to preserve existing mechanisms and develop new ways that allow our different privacy frameworks to co-exist while facilitating the flow of data across borders. The U.S.-EU Safe Harbor Framework, which enables the lawful transfer of personal data from the EU to the U.S., is vital to preserving interoperability.<sup>38</sup>

Most importantly from my perspective, the Safe Harbor provides the FTC with an effective tool to protect the privacy of EU citizens. Our cases against Google, Facebook, and MySpace — which each protect EU consumers as well as American consumers, and together protect 1 billion consumers worldwide — have demonstrated the effectiveness of this Framework, as well as the FTC's determination to enforce it.

In recent months, the NSA revelations have led some to ask whether the Safe Harbor can adequately protect EU citizens' data in the commercial context. My unequivocal answer to this question is "yes." As I said before, the issue of the proper scope of government surveillance is a conversation that should happen — and will happen — on both sides of the Atlantic. But it is a conversation that should proceed outside out of the

---

<sup>36</sup> See FTC Privacy Report, *supra* note 29, at 13.

<sup>37</sup> See WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

<sup>38</sup> See U.S. DEP'T OF COMMERCE, *Safe Harbor Privacy Principles* (Jul. 21, 2000), available at [http://export.gov/safeharbor/eu/eg\\_main\\_018475.asp](http://export.gov/safeharbor/eu/eg_main_018475.asp).

commercial privacy context. In the commercial space, the Safe Harbor Framework facilitates the FTC's ability to protect the privacy of EU consumers. Without the Safe Harbor, my job to protect EU consumers' privacy, where appropriate, would be much harder. In an era where we face many threats to privacy, Safe Harbor has been an effective solution, not the problem.

I understand that Safe Harbor, in part because of its notoriety, is an easy target, but I ask you to consider whether it is the right target. Neither the Safe Harbor nor the EU data protection directive was designed to address national security issues.<sup>39</sup> Data transferred to "adequate" countries, or through binding corporate rules, approved contractual clauses, or the Safe Harbor, are all subject to the same national security exceptions. The most salient difference is that, for transfers made pursuant to Safe Harbor, the FTC is the cop on the beat for commercial privacy issues. The same is not true of the other transfer mechanisms. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection. And, for that reason, I support its continuation.

While some things have changed since my last trip to Brussels in April, many things have remained the same. Our enforcement is still robust, including our enforcement of the Safe Harbor. Our policy development continues. And I believe that the common ground between the U.S. and the EU is still quite fertile.

Last April when I was here I quoted one of my heroes, John F. Kennedy, and I believe it is worth quoting him again. Fifty years ago, in 1963, he said: "[L]et us not be blind to our differences—but let us also direct attention to our common interests and to the means by which those differences can be resolved. And if we cannot end now our differences, at least we can help make the world safe for diversity."<sup>40</sup>

These words continue to ring true – especially now, when we each have so much work to do to foster better consumer privacy protections for all of our citizens.

---

<sup>39</sup> See *id.* See also EU Data Protection Directive, *supra* note 3.

<sup>40</sup> See John F. Kennedy, Commencement Address at American University: Towards a Strategy of Peace (June 10, 1963), available at <http://www.jfklibrary.org/Asset-Viewer/BWC7I4C9QUmLG9J6l8oy8w.aspx>.

# **EXHIBIT**

**11**

**Commissioner Julie Brill's Opening Panel Remarks**  
**European Institute**  
**Data Protection, Privacy and Security:**  
**Re-Establishing Trust Between Europe and the United States**  
**October 29, 2013**

Good morning. I would like to thank Joëlle Attinger and the European Institute for inviting me to speak to you today. I am honored to be here with Jan Philipp Albrecht, Jim Halpert, and our esteemed colleagues from the European Parliament's LIBE committee. Welcome to Washington. I am very happy to say that we are once again open for business.

Your visit comes on the heels of a significant milestone in Brussels. Just last week, the LIBE committee reconciled thousands of amendments to the proposed EU data protection legislation, passed an initial draft, and authorized negotiations with the Council.<sup>1</sup>

In the U.S., we have followed the EU's revision of its privacy framework closely. Although we often hear about the differences between the U.S. and EU privacy frameworks, I think it's important to highlight that we share many of the same goals. The draft EU data protection legislation that the LIBE committee approved last week adopts measures that echo many of the FTC's efforts here in the U.S., including calling on firms to:

- Adopt privacy by design;
- Increase transparency;
- Enhance consumer control;
- Improve data accuracy and consumers' access to their data;
- Strengthen data security;
- Provide parental control over information companies collect about children; and
- Encourage accountability.<sup>2</sup>

As the technological challenges facing the EU and the U.S. have grown, so has our common effort to protect consumers. In some cases, we differ on how to achieve these common goals.<sup>3</sup> For example, we both believe that consent is important, but we have different approaches

---

<sup>1</sup> See Press Release, European Parliament Committee on Civil Liberties, Justice, and Home Affairs, Civil Liberties MEPs pave the way for stronger data protection in the EU (Oct. 21, 2013), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20131021IPR22706%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN>.

<sup>2</sup> See Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), COM (2012) 11 amended (Oct. 21, 2013), available at [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/dv/comp\\_am\\_art\\_01-29/comp\\_am\\_art\\_01-29en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf), [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/dv/comp\\_am\\_art\\_30-91/comp\\_am\\_art\\_30-91en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf) (listing the European Parliament Committee on Civil Liberties, Justice, and Home Affairs's latest amendments to Articles 1-91); FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

as to when and how that consent should be obtained. The particular means we choose may differ, but the challenges we face and our focus on solving them are the same.

Despite our commonalities, recent events make the title of today's discussion – “Re-Establishing Trust Between Europe and the United States” – particularly relevant. There is no doubt that the revelations about the National Security Agency's surveillance programs have severely tested the close friendship between the US and many of our European colleagues. Let me take a moment to address this issue.

Edward Snowden's disclosures about the NSA have sparked a global debate about government surveillance and its impact on individual privacy.<sup>4</sup> There is great interest in the United States and in Europe in having the revelations about the NSA serve as a catalyst for change in the way governments engage in surveillance to enhance national security. As some of you know, I have spent a lifetime working on privacy issues, so it should be no surprise that this is a debate I personally welcome, as my own view is that it is a conversation that is overdue.

But I also think it is important that we have the right conversation — one that is open and honest, practical and productive. As we move forward with this conversation, we should keep in mind that consumer privacy in the commercial sphere, and citizens' privacy in the face of government surveillance to protect national security, are two distinctly separate issues. I and my colleagues at the FTC focus on the appropriate balance between consumer privacy interests and commercial firms' use of consumer data, not on national security issues. And I believe the recent revelations should spur a separate and equally long overdue conversation about how we can further enhance consumer privacy and increase transparency in the commercial sphere.

The FTC is the premier U.S. consumer protection agency focused on commercial privacy. The FTC has a great track record of using its authority to go after unfair or deceptive practices that violate consumer privacy, and vigorously enforcing other laws designed to protect financial<sup>5</sup> and health<sup>6</sup> information, information about children<sup>7</sup>, and credit information used to make decisions about credit, insurance, employment, and housing.<sup>8</sup>

---

<sup>3</sup>See Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Mentor Group Forum for EU-US Legal Economic Affairs: Remarks to the Mentor Group (Apr. 16, 2013), *available at* <http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf>.

<sup>4</sup> See Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (JUN. 9, 2013), *available at* <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

<sup>5</sup> Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.).

<sup>6</sup> Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. 300jj et seq. §§17901 et seq.

<sup>7</sup> Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of companies that operate throughout the Internet and mobile ecosystem. We have brought enforcement actions against well-known companies, such as Google,<sup>9</sup> Facebook,<sup>10</sup> Twitter,<sup>11</sup> and Myspace.<sup>12</sup>

We have also brought myriad cases against companies that are not household names, but whose practices violated the law. We've sued companies that spammed consumers,<sup>13</sup> installed spyware on computers,<sup>14</sup> failed to secure consumers' personal information,<sup>15</sup> deceptively tracked consumers online,<sup>16</sup> violated children's privacy laws,<sup>17</sup> inappropriately collected information on consumers' mobile devices,<sup>18</sup> and failed to secure Internet-connected devices.<sup>19</sup> We have obtained millions of dollars in penalties and restitution in our privacy and data security cases, and placed numerous companies under 20-year orders with robust injunctive provisions.

---

<sup>8</sup> Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x).

<sup>9</sup> In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* <http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf> (decision and order).

<sup>10</sup> In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* <http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf> (decision and order).

<sup>11</sup> In the Matter of Twitter, Inc., FTC File No. 092 3093 (March 3, 2011) *available at* <http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf> (decision and order).

<sup>12</sup> In the Matter of Myspace, LLC, FTC File No. 102 3058 (Aug. 30, 2012) *available at* <http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf> (decision and order).

<sup>13</sup> *See, e.g., FTC v. Flora*, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* <http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf>.

<sup>14</sup> *See, e.g., FTC v. CyberSpy Software, LLC, et al.*, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), *available at* <http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf> (stipulated final order).

<sup>15</sup> *See, e.g., In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), *available at* <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf> (administrative complaint).

<sup>16</sup> *See, e.g., In the Matter of Epic Marketplace, Inc., et al.*, FTC File No. 112 3182 (Dec. 5, 2012), *available at* <http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf> (decision and order).

<sup>17</sup> *See, e.g., U.S. v. Artist Arena, LLC*, No. 12-CV-7386 (S.D.N.Y. Oct. 3, 2012), *available at* <http://www.ftc.gov/os/caselist/1123167/121003artistarenadecree.pdf> (stipulated final order).

<sup>18</sup> *See U.S. v. Path, Inc.*, No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (Consent decree and order), *available at* <http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf>; In the Matter of HTC, Inc., FTC File No. 122 3049 (June 25, 2013), *available at* <http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf> (decision and order).

<sup>19</sup> *See In the Matter of TRENDnet, Inc.*, FTC File No. 122 3090 (Sept. 4, 2013), *available at* <http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf> (agreement containing consent order); *see also* Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement*, N.Y. TIMES, Sept. 8, 2013, *available at* <http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things>.

As a complement to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. In addition to our landmark privacy report issued last year, we have addressed cutting-edge privacy issues involving facial recognition technology,<sup>20</sup> kids apps,<sup>21</sup> mobile privacy disclosures,<sup>22</sup> and mobile payments.<sup>23</sup>

In light of our increasingly interconnected world, the FTC has devoted significant time to enhancing international privacy enforcement cooperation so that we are better able to address global challenges. We continue to foster a strong relationship and engage in ongoing dialogue with European data protection authorities. We meet regularly with EU DPAs, and in April I met with the entire Article 29 Working Party. The Article 29 Working Party has been kind enough to recognize the FTC as a crucial partner in privacy and data protection enforcement.<sup>24</sup> And the Working Party, like the FTC, has welcomed the ongoing dialogue and constructive cooperation between us, and stressed the need for further transatlantic cooperation, especially in enforcement matters, in order to achieve our common goals.<sup>25</sup> Indeed, the FTC's recent Memorandum of Understanding with the Irish DPA establishes a good framework for increased, more streamlined, and more effective privacy enforcement cooperation.<sup>26</sup> And just last month, we worked very closely with our EU and Canadian counterparts to launch the International Conference of Data Protection and Privacy Commissioners' initiative to address challenges in global privacy enforcement cooperation.<sup>27</sup>

---

<sup>20</sup> See Press Release, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), available at <http://ftc.gov/opa/2012/10/facialrecognition.shtm>.

<sup>21</sup> See FED. TRADE COMM'N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012), available at <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf>.

<sup>22</sup> See Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), available at <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>.

<sup>23</sup> See FED. TRADE COMM'N, *Plastic, Paper, or Mobile? An FTC Workshop on Mobile Payments* (March 2013), available at <http://www.ftc.gov/os/2013/03/130306mobilereport.pdf>.

<sup>24</sup> Press Release, Article 29 Data Protection Working Party Meeting with FTC Commissioner Julie Brill (Apr. 29, 2013), available at [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/20130429\\_pr\\_april\\_plenary\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130429_pr_april_plenary_en.pdf).

<sup>25</sup> See *Id.*

<sup>26</sup> Memorandum of Understanding Regarding Mutual Assistance in the Enforcement of Laws Protecting Personal Information in the Private Sector, U.S. FED. TRADE COMM'N-DATA PROTECTION COMMISSIONER OF IRELAND, June 2013, available at <http://www.ftc.gov/os/2013/06/130627usirelandmouprivacyprotection.pdf>.

<sup>27</sup> See Resolution on International Enforcement and Cooperation, 35th International Conference of Data Protection and Privacy Commissioners, Sept. 23-26, 2013, available at <https://privacyconference2013.org/web/pageFiles/kcfinder/files/4.%20Enforcement%20coordination%20resolution%20EN%20.pdf>.

Another critical role played by the FTC is to enforce the U.S.-EU Safe Harbor framework.<sup>28</sup> We know that Safe Harbor has received its share of criticism, particularly in the past few months. We've read the news reports and heard about the recent Parliamentary hearings about Safe Harbor.<sup>29</sup> Given the active debate over Safe Harbor right now, I'd like to address head-on the contention in some quarters that Safe Harbor isn't up to the job of protecting EU citizens' data in the commercial sphere.

First, the FTC vigorously enforces the Safe Harbor. As the Safe Harbor program has grown over the past decade, so has the FTC's enforcement activity. Since 2009, we have brought ten Safe Harbor cases.<sup>30</sup> When Safe Harbor was established, the FTC committed to review on a priority basis all referrals from EU member state authorities.<sup>31</sup> With few referrals over the past decade, we have taken the initiative to proactively look for Safe Harbor violations in every privacy and data security investigation we conduct. That is how we discovered the Safe Harbor violations of Google, Facebook, and Myspace in the last few years. These cases demonstrate the enforceability of Safe Harbor certifications and the high cost that companies can pay for non-compliance. The orders in Google, Facebook, and Myspace require the companies to implement comprehensive privacy programs and subject the companies to ongoing privacy audits for 20 years.<sup>32</sup> Violations of these orders can result in hefty fines, as Google discovered when we assessed a \$22.5 million civil penalty against the company last year for violating its consent decree.<sup>33</sup> The FTC orders against Google, Facebook, and Myspace help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe. These cases demonstrate that Safe Harbor gives the FTC an effective and functioning tool to protect the privacy of EU citizen data transferred to America. Without the Safe Harbor, my job to protect EU consumers' privacy, where appropriate, would be much harder. In an era where we face many threats to privacy, Safe Harbor has been an effective solution, not the problem.

Second, going forward, the FTC will continue to make the Safe Harbor a top enforcement priority. Indeed, we have opened numerous investigations into Safe Harbor compliance in recent months. We will continue to welcome any substantive leads, such as the complaint we received in the past month from a European-based consumer advocate alleging a large number of Safe Harbor-related violations. And, let me be clear, we take this recent complaint very seriously. Of

---

<sup>28</sup> See U.S. DEP'T OF COMMERCE, *Safe Harbor Privacy Principles* (Jul. 21, 2000), available at [http://export.gov/safeharbor/eu/eg\\_main\\_018475.asp](http://export.gov/safeharbor/eu/eg_main_018475.asp).

<sup>29</sup> See *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, Sixth Hearing* (Oct. 7, 2013), available at <http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131014-1500-COMMITTEE-LIBE>.

<sup>30</sup> See Legal Resources, Bureau of Consumer Protection Business Center, U.S. FED. TRADE COMM'N, available at <http://business.ftc.gov/legal-resources/2840/3>.

<sup>31</sup> See Letter from Robert Pitofsky, Chairman, Fed. Trade Comm'n to John Mogg, Director, Directorate-General XV, European Commission (Jul. 14, 2000), available at [http://export.gov/static/sh\\_en\\_FTCLATTERFINAL\\_Latest\\_eg\\_main\\_018455.pdf](http://export.gov/static/sh_en_FTCLATTERFINAL_Latest_eg_main_018455.pdf).

<sup>32</sup> See Google, *supra* note 9; Facebook, *supra* note 10; Myspace, *supra* note 12.

<sup>33</sup> See Press Release, Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), available at <http://ftc.gov/opa/2012/08/google.shtm>.

course, as we do in every instance, we take the necessary time to separate fact from fiction. And, as I am sure many in this audience would appreciate, we also proceed carefully to provide proper notice and appropriate levels of due process. If we discover in our investigations that companies have committed Safe Harbor-related law violations, we will take appropriate enforcement actions.

As I mentioned earlier, I think it is healthy to have a vigorous debate over how to appropriately balance national security and privacy, but that ongoing debate should not be allowed to distort discussions in the commercial sphere about role of the Safe Harbor in protection consumer privacy. The EU itself has created national security exemptions in its existing data protection laws,<sup>34</sup> and the European Commission proposed such exemptions for government surveillance in its draft data protection regulation.<sup>35</sup> In other words, the EU has justifiably recognized the need to tackle their member states' national security issues separately. Safe Harbor is no different and warrants a similar approach. Just as the EU Data Protection Directive was not designed to address national security issues, neither was the Safe Harbor. Whatever the means to transfer data about European consumers for commercial purposes – whether to countries whose laws are deemed “adequate”, through approved contractual clauses, or by way of the Safe Harbor – all these transfer mechanisms are subject to national security exceptions. The difference is that, for Safe Harbor violations, the FTC is the cop on the beat. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection.

I know that some of you in this room may have taken a different view of the Safe Harbor framework. I hope my thoughts give you cause to reexamine the virtues of the Safe Harbor system. As the draft regulation continues its journey through the process of review and adoption, I am hopeful that we can continue to work together to promote both the free flow of data and strong consumer privacy protections.

And while it may not make the headlines or the nightly news, in the midst of all of the recent developments at home and across the pond, our efforts to enhance privacy enforcement cooperation continue to build trust day by day. We want to continue to develop these ties of cross border law enforcement cooperation – including Safe Harbor enforcement – that enhance privacy and data security – as these are the ties that build rather than erode trust, the ties that bind rather than divide us. We have worked extensively with our friends in the EU on these and other issues, and we look forward to continuing that collaboration to enhance privacy protection for consumers on both sides of the Atlantic.

Thank you.

---

<sup>34</sup> Directive 1995/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2005 O.J. (L 281) 31, 42, available at [http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf).

<sup>35</sup> See *Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), available at [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf).

# **EXHIBIT**

**12**

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

FEDERAL TRADE COMMISSION, )

PETITIONER )

v. )

LABMD, INC., )  
and MICHAEL J. DAUGHERTY )

RESPONDENTS )

CIVIL ACTION FILE NO.:  
1:12-CV-3005-WSD

---

County of Cobb

State of Georgia

**AFFIDAVIT OF JOHN W. BOYLE**

The undersigned affiant, John W. Boyle, being first duly sworn, hereby deposes and says:

1. I began employment with LabMD as the VP of Operations and General Manager on November 1, 2006.
2. I am responsible for company-wide operations, which includes the Laboratory, Billing, and IT departments at LabMD.
3. LabMD's primary business is to provide cancer diagnoses through the testing of blood, urine and tissue for physicians.

4. LabMD is a small, privately held medical services company providing uro-pathology and microbiology laboratory services to approximately 70 physician customers. Founded in 1996 by Michael J. Daugherty, President and CEO and 100% corporate shareholder, LabMD operates in a small, specialized medical testing market. The company started in Savannah, Georgia as Southern Diagnostics & Treatment, Inc., and later moved its operations to Atlanta. In 2003, it changed its name to LabMD, Inc.
5. In 2005, LabMD had just six employees for the full year, with an additional ten employees for part of the year; in 2010, it had approximately twenty-four employees for the full year with another seventeen partial year employees.
6. On January 19, 2010, following a brief telephone call to LabMD, the FTC contacted LabMD regarding a “non-public inquiry into LabMD, Inc.’s compliance with federal law governing information security.” A true and correct copy of the January 19, 2010 correspondence (“FTC Inquiry”) is attached hereto as Exhibit A.
7. On February 24, 2010, in response to the FTC Inquiry, LabMD provided a fifteen (15) page detailed response (“February 24 Submission”). The

February 24 Submission included over 5,000 pages of documentation responsive to the FTC's inquiry. A true and correct copy of the February 24 Submission is attached hereto as Exhibit B.

8. On April 28, 2010, as a follow-up to LabMD's detailed written submission, LabMD participated in a detailed telephone conference call with the FTC.
9. On May 6, 2010 the FTC submitted a summary of the April 28, 2010 telephone call to LabMD. A true and correct copy of the May 6, 2010 correspondence is attached hereto as Exhibit C.
10. On June 4, 2010, LabMD supplemented its response to Request 9 and included a copy of LabMD's Computer Hardware, Software and Data Usage and Security Policy Manual. A true and correct copy of the June 4, 2010 correspondence is attached hereto as Exhibit D.
11. On July 16, 2010, LabMD again supplemented its response with a written narrative timeline of LabMD's ongoing audits, activities, assessments and security measures implemented by LabMD and 617 bates labeled documents. A true and correct copy of the July 16, 2010 correspondence is attached hereto as Exhibit E.
12. On July 23, 2010, LabMD met in person with the FTC to discuss its inquiry. Present at the meeting were the President and CEO of LabMD, Michael J.

Daugherty, the Vice-President of Operations and General Manager of LabMD, John Boyle, and LabMD's outside general counsel at the time, Ms. Philippa Ellis. Mr. Alain Sheer and Ms. Ruth Yodaiken were present from the FTC and conducted an exhaustive inquiry into LabMD's previous submissions, the operations of LabMD and the specific details related to its January 19, 2010 Inquiry.

13. Following the detailed in-person inquiry, LabMD again supplemented its responses to the FTC Inquiry based upon the oral examination of Mr. Daugherty and Mr. Boyle and for a fifth time, on August 30, 2010, LabMD responded in written narrative form to the FTC's Inquiry regarding written policies and measures and provided 925 pages of documents to the FTC. A true and correct copy of the August 30, 2010 submission is attached hereto as Exhibit F.

14. On February 23, 2011, the FTC contacted LabMD to conduct an investigational hearing to obtain additional information about the information security policies, procedures and practices LabMD implemented between January 1, 2009 and August 30, 2010. A true and correct copy of the February 23, 2011 correspondence is attached hereto as

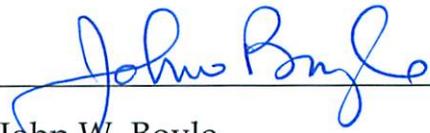
Exhibit G. This request for an investigative statement was withdrawn by the FTC on its own accord.

15. On May 16, 2011, LabMD submitted an eight page written narrative with 24 exhibits and 169 pages of supplemental materials. A true and correct copy of the May 16, 2011 correspondence is attached hereto as Exhibit H.

16. LabMD further clarified certain issues raised in the May 16, 2011 submission on May 31, 2011 in a six page written submission with 14 additional exhibits. A true and correct copy of May 31, 2011 written submission is attached hereto as Exhibit I.

17. To date, LabMD has incurred in excess of \$100,000.00 in costs to comply with the FTC's inquiry.

This the 14th day of September, 2012.

  
\_\_\_\_\_  
John W. Boyle

Sworn and subscribed before me this  
the 14th day of September, 2012.

  
\_\_\_\_\_

Notary Public

My Commission expires: May 12, 2014

PATRICIA GILBRETH  
NOTARY PUBLIC  
FORSYTH COUNTY GEORGIA  
My Commission Expires  
May 12, 2014

# **EXHIBIT**

**13**

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:** Deborah Platt Majoras, Chairman  
Pamela Jones Harbour  
Jon Leibowitz  
William E. Kovacic  
J. Thomas Rosch

**RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC  
INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY  
AND/OR DATA SECURITY**

File No. P954807

**Nature and Scope of Investigation:**

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

**Authority to Conduct Investigation:**

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; FTC Procedures and Rules of Practice, 16 C.F.R. 1.1 *et seq.* and supplements thereto.

By direction of the Commission.

  
Donald S. Clark  
Secretary

Issued: January 3, 2008

# **EXHIBIT**

**14**

**Dissenting Statement of Commissioner J. Thomas Rosch**  
Petitions of LabMD, Inc. and Michael J. Daugherty  
to Limit or Quash the Civil Investigative Demands

FTC File No. 1023099  
June 21, 2012

I dissent from the Commission's vote affirming Commissioner Brill's letter decision, dated April 20, 2012, that denied the petitions of LabMD, Inc. and Michael J. Daugherty to limit or quash the civil investigative demands.

I generally agree with Commissioner Brill's decision to enforce the document requests and interrogatories, and to allow investigational hearings to proceed. As she has concluded, further discovery may establish that there is indeed reason to believe there is Section 5 liability regarding petitioners' security failings *independent* of the "1,718 File" (the 1,718 page spreadsheet containing sensitive personally identifiable information regarding approximately 9,000 patients) that was originally discovered through the efforts of Dartmouth Professor M. Eric Johnson and Tiversa, Inc. In my view, however, as a matter of prosecutorial discretion under the unique circumstances posed by this investigation, the CIDs should be limited. Accordingly, without reaching the merits of petitioners' legal claims, I do not agree that staff should further inquire – either by document request, interrogatory, or investigational hearing – about the 1,718 File.

Specifically, I am concerned that Tiversa is more than an ordinary witness, informant, or "whistle-blower." It is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations. Indeed, in the instant matter, an argument has been raised that Tiversa used its robust, patented peer-to-peer monitoring technology to retrieve the 1,718 File, and then repeatedly solicited LabMD, offering

investigative and remediation services regarding the breach, long before Commission staff contacted LabMD. In my view, while there appears to be nothing *per se* unlawful about this evidence, the Commission should avoid even the appearance of bias or impropriety by not relying on such evidence or information in this investigation.

# **EXHIBIT**

**15**



UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

RXZ

Bureau of Consumer Protection  
Division of Advertising Practices

Carl H. Settlemyer, III  
202 326 2019 (Direct)  
202 326 3259 (Fax)  
csettlemyer@ftc.gov

June 25, 2008

**VIA EMAIL AND REGULAR MAIL**

Robert Boback, Chief Executive Officer  
Tiversa, Inc.  
144 Emeryville Drive, Suite 300  
Cranberry Township, PA 16066

Dear Mr. Boback:

This notifies you of an official request for information that the Federal Trade Commission has received from Chairman Waxman of the Committee on Oversight and Government Reform of the House of Representatives. The Committee has requested information concerning inadvertent file sharing over peer-to-peer ("P2P") networks. Certain information and materials that Tiversa submitted may be responsive to this request.

The Commission routinely receives official requests for confidential information from congressional committees and subcommittees. Neither the Freedom of Information Act, 5 U.S.C. § 552(d), nor the Federal Trade Commission Act, 15 U.S.C. § 57b-2(d)(1)(A), authorize the Commission to withhold such information from congressional committees or subcommittees. The Commission, of course, requests that the responsive information and materials be kept confidential by the congressional committees and subcommittees.

If you have any questions about the Committee's inquiry or handling of information it has requested, please direct them to Committee staff contact, Roger Sherman, at (202) 225-5051. Questions about the Commission's response may be directed to me at (202) 326-2019.

Sincerely,

A handwritten signature in black ink, appearing to read "Carl H. Settlemyer".

Carl H. Settlemyer

cc: Office of General Counsel

RX5

**Kelly, Andrea**

---

**From:** Robert Boback <rboback@tiversa.com>  
**Sent:** Wednesday, March 04, 2009 5:26 PM  
**To:** Settlemyer, Carl  
**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** RE: P2P ID Theft Reseach - Conference Call?

The main office number will be fine. Its listed below.

Talk to you tomorrow.

Best,  
Bob

Robert Boback  
*Chief Executive Officer*

**Tiversa, Inc.**  
*The P2P Intelligence Experts*  
144 Emeryville Drive, Suite 300  
Cranberry Township, Pennsylvania 16066  
| 724-940-9030 Office | 724-940-9033 Fax

---

**From:** Settlemyer, Carl [mailto:csettlemyer@ftc.gov]  
**Sent:** Wednesday, March 04, 2009 5:28 PM  
**To:** Robert Boback  
**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** RE: P2P ID Theft Reseach - Conference Call?

That's fine, Bob. Looking forward to it.

For now, we'll plan to call you from one of our conference rooms. We may, however, set up a call in number if it helps one of our folks participate in the call. We'll let you know. What number should we call?

Thanks.

Carl S.

---

**From:** Robert Boback [mailto:rboback@tiversa.com]  
**Sent:** Wednesday, March 04, 2009 5:20 PM  
**To:** Settlemyer, Carl  
**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** RE: P2P ID Theft Reseach - Conference Call?

Carl,

Noon would work better on this end. I pushed a separate lunch meeting back to 12:45. Hopefully that will work on your end.

Best,

Bob

Robert Boback  
*Chief Executive Officer*

**Tiversa, Inc.**  
*The P2P Intelligence Experts*  
144 Emeryville Drive, Suite 300  
Cranberry Township, Pennsylvania 16066  
| 724-940-9030 Office | 724-940-9033 Fax

---

**From:** Settlemyer, Carl [mailto:csettlemyer@ftc.gov]  
**Sent:** Wednesday, March 04, 2009 3:46 PM  
**To:** Robert Boback  
**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** RE: P2P ID Theft Reseach - Conference Call?

Bob:

That would be great. 12:30 would be the best time for us, from a scheduling standpoint, but we could do the call any time in the noon-2pm window. I think a half hour would suffice. Please let us know what would work best for you.

Thanks.

Carl S.

---

**From:** Robert Boback [mailto:rboback@tiversa.com]  
**Sent:** Wednesday, March 04, 2009 1:55 PM  
**To:** Settlemyer, Carl  
**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** RE: P2P ID Theft Reseach - Conference Call?

Carl,

I have time on tomorrow (3/5) for a call but I will be out of the office on Friday. Please let me know if you have some time tomorrow.

Best Regards,  
Bob

Robert Boback  
*Chief Executive Officer*

**Tiversa, Inc.**  
*The P2P Intelligence Experts*  
144 Emeryville Drive, Suite 300  
Cranberry Township, Pennsylvania 16066  
| 724-940-9030 Office | 724-940-9033 Fax

---

**From:** Settlemyer, Carl [mailto:csettlemyer@ftc.gov]  
**Sent:** Monday, March 02, 2009 5:28 PM  
**To:** Robert Boback

**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** RE: P2P ID Theft Reseach - Conference Call?

Bob:

Do you any free time to talk on Friday morning? Most of us appear to be free on Thursday morning if that would work better for you. Any time after 9:30 or 10 would probably work fine for us. Obviously we'd also like to discuss (to the extent you are free to do so) the incident that broke over the weekend.

Thanks.

Carl S.

---

**From:** Robert Boback [mailto:rboback@tiversa.com]  
**Sent:** Tuesday, February 24, 2009 12:24 PM  
**To:** Settlemyer, Carl  
**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** RE: P2P ID Theft Reseach - Conference Call?

Ok

Robert Boback  
*Chief Executive Officer*

**Tiversa, Inc.**  
*The P2P Intelligence Experts*  
144 Emeryville Drive, Suite 300  
Cranberry Township, Pennsylvania 16066  
| 724-940-9030 Office | 724-940-9033 Fax

---

**From:** Settlemyer, Carl [mailto:csettlemyer@ftc.gov]  
**Sent:** Tuesday, February 24, 2009 11:45 AM  
**To:** Robert Boback  
**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** RE: P2P ID Theft Reseach - Conference Call?

Bob:

No problem. We are sure you are quite busy. We are still interested in speaking with you. I'll check with my colleagues and see if any days later this week or early next week might be viable and get back to you ASAP.

Thanks.

Carl S.

---

**From:** Robert Boback [mailto:rboback@tiversa.com]  
**Sent:** Tuesday, February 24, 2009 11:36 AM  
**To:** Settlemyer, Carl  
**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** RE: P2P ID Theft Reseach - Conference Call?

Carl,

I hope this email finds you doing well. I apologize for the delay in my responding to this email. If you are still interested in a call, please let me know.

Best Regards,  
Bob

Robert Boback  
*Chief Executive Officer*

**Tiversa, Inc.**  
*The P2P Intelligence Experts*  
144 Emeryville Drive, Suite 300  
Cranberry Township, Pennsylvania 16066  
| 724-940-9030 Office | 724-940-9033 Fax

---

**From:** Settlemyer, Carl [mailto:csettlemyer@ftc.gov]  
**Sent:** Monday, January 26, 2009 11:34 AM  
**To:** Robert Boback; Chris Gormley  
**Cc:** Ferguson, Stacey; Sheer, Alain; Quaresima, Richard A.  
**Subject:** P2P ID Theft Reseach - Conference Call?

Bob and Chris:

We hope you are well. We saw Tiversa's press release last week about some new research that you've done. We were hoping you might have some time to discuss that with us in a conference call next week. Other than Thursday afternoon, our calendars next week look relatively clear, so we could probably be available anytime that is convenient for you.

We look forward to speaking with you.

Regards,

Carl S.

Carl H. Settlemyer, Attorney  
Federal Trade Commission  
BCP-Division of Advertising Practices  
600 Pennsylvania Ave., N.W., Room NJ-3212  
Washington, DC 20580  
Tel: 202-326-2019  
csettlemyer@ftc.gov

# **EXHIBIT**

**16**

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION

\_\_\_\_\_)  
IN THE MATTER OF )  
 )  
LabMD Inc. )  
 )  
\_\_\_\_\_)



**LabMD'S PETITION TO LIMIT OR  
QUASH THE CIVIL INVESTIGATIVE DEMAND**

Claudia Callaway, Esq.  
Christina Grigorian, Esq.  
Julian Dayal, Esq.  
Katten Muchin Rosenman LLP

2900 K Street, NW  
North Tower - Suite 200  
Washington, DC 20007  
Phone: (202) 625-3613  
Facsimile: (202) 298-7570  
Email: [claudia.callaway@kattenlaw.com](mailto:claudia.callaway@kattenlaw.com)

*Counsel for Petitioner*

**Table of Contents**

	<u>Page</u>
I. FACTUAL SUMMARY .....	1
A. The 1,718 File Was Illegally Downloaded By Tiversa, Inc., A Technology Corporation Using Patented Computer Technology, With The Support Of Federally-Funded Researchers At Dartmouth College .....	2
B. Petitioner’s Lawsuit Against Tiversa and Dartmouth College .....	4
II. ARGUMENT .....	5
A. The FTC’s Authority Under Section 45.....	5
B. There Is No Basis Under Section 45 To Support Enforcement Of The Present CID, Which Is In All Events Exceedingly Overbroad And Unduly Burdensome .....	7
C. The CID Should Be Quashed Because It Is Not Authorized by A Valid Resolution And Is Therefore Indefinite, Overbroad, And Incapable Of Demonstrating A Valid Exercise Of The FTC’s Section 45 Authority.....	10
D. The CID Improperly Demands Documents And Testimony Concerning Matters That Are Primarily Regulated By The Department Of Health And Human Services .....	12
III. CONCLUSION.....	13

**LabMD'S PETITION TO QUASH  
THE CIVIL INVESTIGATIVE DEMAND**

Petitioner LabMD Inc. hereby petitions the Federal Trade Commission ("FTC"), pursuant to 16 C.F.R. § 2.7(d), to quash the Civil Investigative Demand ("CID") issued to Petitioner on December 21, 2011. The FTC issued the CID pursuant to its alleged authority under Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1 and therein makes various demands, including the production of all documents related to any "security risk, vulnerability, and incidents through which [Petitioner's] documents and information [] either were or could have been disclosed to unrelated third parties."<sup>1</sup> Petitioner respectfully submits that the FTC lacks the authority to issue the CID in its entirety to LabMD. Accordingly, Petitioner respectfully petitions the Commission to quash the CID.<sup>2</sup>

**I. FACTUAL SUMMARY**

Although the present CID is worded in the broadest possible manner, it appears to be premised on the third-party download of a single document belonging to Petitioner (the "1,718 File"). The 1,718 File, which contained personally identifiable information ("PII") and protected health information ("PHI") about some of Petitioner's patients, was illegally downloaded from Petitioner's computers in February of 2008. To Petitioner's knowledge, no other incidents such as this have occurred, nor does the CID reference or allege any additional incidents (despite the absence of any limitation to the CID's testimonial and documentary requests). Therefore, and because there is no other conceivable basis for the CID, Petitioner sets forth the facts

---

<sup>1</sup> A true and correct copy of the December 21, 2011 Civil Investigative Demand is attached hereto as Exhibit A.

<sup>2</sup> This petition to quash is based on the FTC's lack of authority to issue a CID to LabMD on the basis of the 1,718 File incident. However, Petitioner explicitly reserves any and all arguments or claims concerning the CID itself in the event that the FTC is found to have the requisite authority to issue a CID targeting LabMD on the basis of the 1,718 File incident.

surrounding the 2008 download of the 1,718 File, all of which are part of the FTC's private investigation record and/or are currently being adjudicated by a federal court in a civil action that Petitioner brought against the parties who illegally downloaded the 1,718 File.

**A. The 1,718 File Was Illegally Downloaded By Tiversa, Inc., A Technology Corporation Using Patented Computer Technology, With The Support Of Federally-Funded Researchers At Dartmouth College**

Tiversa, Inc. is a Pennsylvania Corporation who provides peer-to-peer ("P2P") intelligence services to corporations, government agencies, and individuals based on its patented EagleVision X1 technology that can monitor over 550 million computer users daily.<sup>3</sup> On information and belief, both Tiversa and its partner, Dartmouth College, accepted federal funds from the National Institute of Standards and Technology, the United States Department of Justice, the United States of Homeland Security, and the National Science Foundation, among other governmental agencies, to develop P2P search technology. During a 2007 congressional hearing, Tiversa testified that its proprietary technology allowed it to process 300 million searches per day, or over 170 million more searches than Google was processing per day.<sup>4</sup> At the same hearing, Tiversa admitted that it had downloaded computer files containing, but by no means limited to –

federal and state identification, including passports, driver's license, Social Security cards, dispute letters with banks, credit card companies, insurance companies, copies of credit reports--Experian, TransUnion, Equifax, Individual bank card statements and credit card statements, signed copies of health insurance cards, full copies of tax returns, active user names and passwords for online banking and brokerage accounts and confidential medical histories and records.<sup>5</sup>

---

<sup>3</sup> See Company Overview, Website for Tiversa, <http://www.tiversa.com/about/>.

<sup>4</sup> See Tiversa's July 24, 2007 testimony before the United States House of Representatives Committee on Oversight and Government Reform, a true and correct copy of which is attached hereto as Exhibit B, at 3.

<sup>5</sup> *Id.* at 5.

Two years later, in April of 2009, Dartmouth College published a paper entitled *Data Hemorrhage in the Health-Care Sector*.<sup>6</sup> The paper was based upon activities “conducted in collaboration with Tiversa” using Tiversa’s proprietary technology<sup>7</sup> and was financially supported by a U.S. Department of Homeland Security Grant Award issued under the auspices of the Institute for Information Infrastructure Protection.<sup>8</sup> According to the paper, Tiversa and Dartmouth began their project by “looking for files from top ten publicly traded health-care firms” that were available on P2P networks.<sup>9</sup> As part of the initial search, Tiversa and Dartmouth manually reviewed 3,328 computer files downloaded from P2P networks, many of which contained PII and PHI.<sup>10</sup>

Following their initial search, Tiversa and Dartmouth undertook a second search (“Second Search”) lasting approximately six months.<sup>11</sup> During the Second Search, Tiversa and Dartmouth downloaded closed to four million documents, including over 20,000 medical patient records.<sup>12</sup> Tiversa described the evolving technology it used for the Second Search in a 2009 hearing before the United States House of Representatives Subcommittee on Commerce, Trade and Consumer Protection (“2009 CTC hearing”). Tiversa testified that, through the use of its proprietary software, it “can see and detect all previously undetected activity” and “where an individual user can only see a very small portion of a P2P file sharing network, [it] can see the

---

<sup>6</sup> A true and correct copy of the April 2009 paper is attached hereto as Exhibit C.

<sup>7</sup> *Id.* at 1.

<sup>8</sup> *Id.*

<sup>9</sup> *Id.* at 8.

<sup>10</sup> *Id.* at 9-11.

<sup>11</sup> *Id.* at 11.

<sup>12</sup> *Id.* at 13 (referencing the 20,000 medical patient records that were downloaded); *see also* Tiversa’s May 4, 2009 testimony before the United States House of Representatives Subcommittee on Commerce, Trade and Consumer Protection, a true and correct copy of which is attached hereto as Exhibit D, at 10 (referencing the nearly four million documents that were downloaded).

P2P network in its entirety in real time.”<sup>13</sup> Further, Tiversa “processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day”.<sup>14</sup> To showcase its technology, during the hearing Tiversa, performed a “live demonstration” whereby it intentionally searched for and downloaded over 275,000 tax returns.<sup>15</sup>

On July 29, 2009, Tiversa appeared before the United States House of Representatives Committee on Oversight and Government Reform and testified further about the technology it had used to perform the Second Search.<sup>16</sup> According to its testimony, Tiversa deployed newly developed P2P search technology that allowed it to penetrate even “the most technologically advanced” computer security despite the presence of “firewalls and encryption.”<sup>17</sup> It was with this technology, and during the Second Search, that Tiversa and Dartmouth downloaded the 1,718 File, a copy of which Tiversa produced at the 2009 CTC hearing.<sup>18</sup>

#### **B. Petitioner’s Lawsuit Against Tiversa and Dartmouth College**

Rather than agreeing to destroy its copies of the 1,718 File or explain to Petitioner how it had downloaded the 1,718 File, Tiversa solicited Petitioner on six occasions to purchase its security services in order to “remediate” any issues involving the 1,718 File.<sup>19</sup> For example, on May 15, 2008, Tiversa informed Petitioner that any information regarding the means by which it acquired the 1,718 File “would require a professional services agreement.”<sup>20</sup> Dartmouth,

---

<sup>13</sup> Ex. D at 3-4.

<sup>14</sup> *Id.* at 4.

<sup>15</sup> *Id.*

<sup>16</sup> A true and correct copy of Tiversa’s July 29, 2009 testimony before the United States House of Representatives Committee on Oversight and Government Reform is attached hereto as Exhibit E.

<sup>17</sup> Ex. E at 3.

<sup>18</sup> Ex. B at 11.

<sup>19</sup> *See infra* note 22, Ex. F at ¶¶ 72-98.

<sup>20</sup> *Id.* at ¶ 87.

meanwhile, used federal funding to publish at least two additional papers discussing the activities leading to the download of the 1,718 File.<sup>21</sup>

On November 23, 2011, Petitioner filed suit against Tiversa and Dartmouth alleging, among other things, computer fraud, computer crimes, conversion, and trespass.<sup>22</sup> Tiversa, with the support of Dartmouth, was and is running an extortionist scheme whereby it uses its government-funded technology to penetrate computer networks, download confidential files, and then sell the files back to the owners under the guise of providing network security.

## II. ARGUMENT

### A. The FTC's Authority Under Section 45

While 15 U.S.C. § 45(a) grants the FTC the authority to investigate deceptive or unfair practices affecting commerce, this authority is not without limits. Likewise, although Congress has empowered the FTC under Section 57b-1 to issue CIDs in support of investigations undertaken pursuant to Section 45, a CID is only enforceable to the extent it rests on a legitimate exercise of Section 45 authority. In part for this reason, CIDs are not self-enforcing and the target of a CID is entitled to judicial review of a CID to prevent misuse of the FTC's statutory authority.<sup>23</sup>

In *U.S. v. Morton Salt Co.*, the United States Supreme Court established the standard for determining when a CID should be quashed.<sup>24</sup> Although the Court enforced the decree at issue in

---

<sup>21</sup> *Id.* at ¶¶ 100-102.

<sup>22</sup> *LabMD Inc. v. Tiversa, Inc.*, No 1:11-cv-4044 (Nov. 30, 2011 N.D. Ga.). A true and correct copy of the Complaint is attached hereto as Exhibit F.

<sup>23</sup> *See, e.g., SEC v. Arthur Young & Co.*, 584 F.2d 1018, 1024 (D.C. Cir. 1978), *cert denied*, 439 U.S. 1071 (1979) ("The federal courts stand guard, of course, against abuses of their subpoena-enforcement processes . . .") (citing *U.S. v. Powell*, 379 U.S. 48, 58 (1964) and *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186,216 (1946)); *D.R. Horton, Inc. v. Jon Leibowitz, Chairman*, No. 4:IO-CV-547-A, 2010 WL 4630210, at \*2 (N.D. Tex. Nov. 3, 2010). ("As the government notes in its motion documents, the CID is not self-executing, and may only be enforced by a district court in an enforcement proceeding.")

<sup>24</sup> 338 U.S. 632 (1950).

that case, it recognized that “a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power” of the agency.<sup>25</sup> Accordingly, the Court held that agency subpoenas or CIDs should not be enforced if they demand information that is: (a) not “within the authority of the agency,” (b) “too indefinite,” or (c) not “reasonably relevant to the inquiry.”<sup>26</sup> This standard has been consistently applied by the federal judiciary.<sup>27</sup> For example, in *SEC v. Blackfoot Bituminous, Inc.*, the Court of Appeals for the Tenth Circuit confirmed that “an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met”.<sup>28</sup>

The costs and burdens imposed by a CID must also be considered.<sup>29</sup> An administrative agency may not use its investigative powers to go on a fishing expedition.<sup>30</sup> Rather, a CID must be based on a justifiable belief that wrongdoing has actually occurred. The Supreme Court did

---

<sup>25</sup> *Id.* at 652

<sup>26</sup> *Id.*

<sup>27</sup> *See, e.g., SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d 512 (10th Cir. 1980) (citing *Morton Salt*, 338 U.S. at 653) (confirming that “to obtain judicial enforcement of an administrative subpoena, an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met”).

<sup>28</sup> *Id.* at 514; *see also Arthur Young & Co.*, 584 F.2d at 1030-31 (noting that a subpoena request must “not [be] so overbroad as to reach into areas that are irrelevant or immaterial” and that specifications must not exceed the purpose of the relevant inquiry) (internal quotation marks and citation omitted); *FTC v. Mt. Olympus Fin. LLC*, 211 F.3d 1278 (10th Cir. 2000) (“the documents requested were reasonably relevant to an inquiry clearly within the authority of the FTC”); *United States v. Construction Prods. Research, Inc.*, 73 F.3d 464, 471 (2d Cir. 1996) (stating that “the disclosure sought must always be reasonable”); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1089 (D.C. Cir. 1993) (holding that a CID is enforceable only “if the information sought is reasonably relevant”); *FTC v. Texaco, Inc.*, 555 F.2d 862, 881 (D.C. Cir. 1977) (stating that the “the disclosure sought shall not be unreasonable”).

<sup>29</sup> *See, e.g., FTC v. Texaco, Inc.*, 555 F.2d 862, 882 (D.C. Cir. 1977) (a party challenging a subpoena can successfully do so on the grounds that compliance would be overly burdensome or unreasonable); *see also Phoenix Bd. Of Realtors, Inc. v. Dep't of Justice*, 521 F. Supp. 828, 832 (D. Ariz. 1981) (the government should narrow the scope of a CID when compliance may be overly burdensome).

<sup>30</sup> *See FDIC v. Garner*, 126 F.3d 1138, 1146 (9th Cir. 1997); *FTC v. Nat'l Claims Serv., Inc.*, No. S. 98-283, 1999 WL 819640, at \* 1 (E.D. Cal. Feb. 9, 1999). *See also* S. Rep. 96-500 at 4, 96th Congress 1st Session (1979) (“The FTC’s broad investigatory powers have been retained but modified to prevent fishing expeditions undertaken merely to satisfy its ‘official curiosity.’”).

not equivocate in *FTC v. Am. Tobacco Co.* when it made clear that “[i]t is contrary to the first principles of justice to allow a search through all the respondents’ records, relevant or irrelevant, in the hope that something will turn up.”<sup>31</sup> And, of course, the mere fact that a party has suffered a data security incident does not imply any wrongdoing on the part of the victimized party.<sup>32</sup> That is especially so when (as here) there are no allegations that the petitioner violated any established public policy or that petitioner’s customers suffered any injury as a result of the data incident.<sup>33</sup>

**B. There Is No Basis Under Section 45 To Support Enforcement Of The Present CID, Which Is In All Events Exceedingly Overbroad And Unduly Burdensome**

In the present case, there is no basis under Section 45 for imposing a highly burdensome CID upon Petitioner to investigate either 1) the download of the 1,718 File by Tiversa and Dartmouth specifically or, 2) Petitioner’s data security generally. As an initial matter, Tiversa and Dartmouth’s use of government-funded, highly-proprietary, and patented technology which according to Tiversa’s congressional testimony can penetrate even the most robust network security<sup>34</sup> to download the 1,718 File in February of 2008 cannot conceivably amount to an unfair or deceptive practice on the part of Petitioner. Indeed, according to Tiversa

---

<sup>31</sup> 264 U.S. 298,306 (1924).

<sup>32</sup> See, e.g., Holly K. Towle, Let’s Play “Name that Security Violation!”, 11 *Cyberspace Lawyer*, Apr. 2006, at 11.

<sup>33</sup> “Unjustified consumer injury is the primary focus of the FTC Act.” Unfairness Statement, 104 F.T.C. 949, 1073 (1984); see also *id.* at 1076 (if a public policy is not well-established, the agency will “act only on the basis of convincing independent evidence that the practice was distorting the operation of the market and thereby causing unjustified consumer injury”).

<sup>34</sup> Ex. E at 3, 6, 8 (concluding that “the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies”).

itself, the security issues enabling the download of the 1,718 File were not unique to Petitioner, but were common to almost every networked computer in the country.<sup>35</sup>

Likewise, the FTC cannot point to any public policy existing in February of 2008 that Petitioner violated, thereby enabling Tiversa and Dartmouth to download the 1,718 File. To date, the FTC has not enacted any rules or standards regarding issues associated with P2P networks, which is the FTC's most common remedy for problematic issues "that occur on an industry-wide basis."<sup>36</sup> And it was not until 2010 that the FTC began notifying organizations that failure to take adequate steps to protect against the security issues posed by P2P networks could result in liability under federal law.<sup>37</sup> 2010 was also the year in which the FTC first published *Peer-to-Peer File Sharing: A Guide for Business*.<sup>38</sup> Thus, by all accounts, the present CID seeks to hold Petitioner's 2008 conduct to a standard of perfect security, a standard that the FTC itself has made clear is impossible to attain.<sup>39</sup> This is not only unfair and unreasonable, but it grossly exceeds the FTC's authority under Section 45 to investigate unfair and deceptive practices as the 2008 download of the 1,718 File by Tiversa and Dartmouth is evidence of neither.

And yet, based apparently on nothing more than possession of the 1,718 File, the CID seeks, among other things, production within 30 days of all documents relating in any manner to

---

<sup>35</sup> *Id.*

<sup>36</sup> A Brief Overview Of The Federal Trade Commission's Investigative And Law Enforcement Authority, July 2008, Section II(b), *available at* <http://www.ftc.gov/ogc/brfovrw.shtm>.

<sup>37</sup> *See FTC Warns of Breach Risk From P2P File-Sharing*, 9 No. 3 Employer's Guide HIPAA Privacy Requirements Newsl. 4 (Apr. 2010).

<sup>38</sup> *Available at* <http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business>.

<sup>39</sup> *See* Statement of the Federal Trade Commission Before the House Subcomm. on Technology, Information Policy, Intergovernmental Relations, and the Census, Comm. on Government Reform (Apr. 21, 2004) at 4 ("The Commission recognized that there is no such thing as 'perfect' security and that breaches can occur even when a company has taken all reasonable precaution."), *available at* <http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf>. *See also* Deborah Platt Majoras, *The Federal Trade Commission: Learning from History as We Confront Today's Consumer Challenges*, 75 UMKC L. Rev. 115, 128 (2006) ("The laws and rules we enforce do not require that information security be perfect. Such a standard would be costly and unobtainable.").

all of Petitioner's security practices and policies (without temporal limitation). This is not only unduly burdensome, and therefore unenforceable,<sup>40</sup> but the overwhelming majority of documents related to Petitioner's security practices and policies, past and present, have nothing to do with the 2008 download of the 1,718 File. There is absolutely no basis for using the 1,718 File download as a springboard to conduct a costly and burdensome fishing expedition into Petitioner's security practices and procedures.<sup>41</sup>

The FTC's timing here is also troubling. The 2008 download of the 1,718 File was explicitly reviewed by at least two congressional committees (none of which recommended taking any course of action against Petitioner). And yet, in the three years since the download of the 1,718 File was publicized in the chambers of the Congress and elsewhere, the FTC took no action. It wasn't until Petitioner declined to engage Tiversa for "security services" for the sixth time and then sued Tiversa for theft and extortion that the FTC was compelled to issue the present CID. This unusual timing only serves to incentivize organizations to pay off Tiversa (as non-payment appears to coincide with the opening of an FTC investigation).

Taken together, the present CID vastly exceeds the FTC's authority under Section 45. The government funded download of the 1,718 File in 2008 by Tiversa and Dartmouth manifestly fails to provide any evidence whatsoever of any unfair or deceptive practice by Petitioner. Consequently, the 1,718 File download (and the facts surrounding the download) not only does not provide a basis for a further FTC investigation into the download itself vis-a-vis

---

<sup>40</sup> See *FTC v. Texaco, Inc.*, 555 F.2d at 882) (respondent should not have "to cull its files for data" that would "impose and undue burden" and finding that a subpoena requiring production of "all documents that in any way reference" the issue in question "would be unduly burdensome").

<sup>41</sup> When a CID makes demands "of such a sweeping nature and so unrelated to the matter properly under inquiry" such that they are not "reasonably relevant", they should not be enforced. See *Morton Salt Co.* 228 U.S. at 652; see also *In re Sealed Case (Administrative Subpoena)*, 42 F.3d 1412, 1420 (D.C. Cir. 1994) (remanding to the district court to determine whether the information requested related to a "valid purpose" of the agency's investigation).

Petitioner, but it emphatically does not provide any basis for a deeply burdensome, open-ended investigation into all of Petitioner's past and present security practices and procedures. As a result, the present CID should be quashed.

**C. The CID Should Be Quashed Because It Is Not Authorized by A Valid Resolution And Is Therefore Indefinite, Overbroad, And Incapable Of Demonstrating A Valid Exercise Of The FTC's Section 45 Authority**

Under 16 C.F.R. § 2.6, "any person under investigation compelled or requested to furnish information or documentary evidence shall be advised of the purpose and scope of the investigation and of the nature of the conduct constituting the alleged violation which is under investigation and the provisions of law applicable to such violation." Courts assess the validity of a CID by looking to the purpose and scope of the investigation and the nature of the conduct constituting the alleged violation as stated in the authorizing resolution.<sup>42</sup> Importantly, however, a court can look only to the resolutions (and not any outside communications) to evaluate the scope of an investigation.<sup>43</sup> Accordingly, the FTC Operating Manual provides that –

Investigational resolutions must adequately set forth the nature and scope of the investigation. The statement may be brief, but it must be specific enough to enable a court in an enforcement action to determine whether the investigation is within the authority of the Commission and the material demanded by the compulsory process is within the scope of the resolution.<sup>44</sup>

The single resolution that purportedly supports the present CID utterly fails the FTC's own rules and operational requirements. The resolution states, in its entirety, that "the nature and scope" of the FTC's investigation is –

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended.

---

<sup>42</sup> See, e.g., *F.T.C. v. Carter*, 636 F.2d 781,789 (D.C. Cir. 1980).

<sup>43</sup> See, e.g., *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1088 (D.C. Cir. 1992).

<sup>44</sup> O.M.3.3.6.7.4.1.

Such investigation shall, in addition, determine whether the Commission action to obtain redress of injury to consumers or others would be in the public interest.

This resolution is so sweeping that it would allow the Commission to investigate any person or entity with respect to anything. Such a broad resolution is inconsistent with both 16 C.F.R. § 2.6 and the statutory resolution requirement in 15 U.S.C. § 57b-1(i).<sup>45</sup>

In upholding a resolution that was far more specific than the resolution here, the D.C. Circuit made clear that there are limits to the FTC's use of broad, non-specific resolutions. Under the D.C. Circuit's standard, the present resolution is utterly inadequate:

The Commission equaled this standard, and allowed our examination of the relevance of their subpoena requests, by identifying the specific conduct under investigation cigarette advertising and promotion and specific statutory provisions that confer authority and duties upon the Commission. Section 8(b) of the Cigarette Labeling and Advertising Act, under which the Commission must report to Congress on the effectiveness of cigarette labeling and current practices and methods of cigarette advertising and promotion, is self-expressive of several purposes of this investigation. We can therefore say that recitation of the statutory authority itself alerts the respondents to the purposes of the investigation. ***Section 5's prohibition of unfair and deceptive practices, which, standing broadly alone would not serve very specific notice of purpose***, is defined by its relationship to section 8(b), as is the extremely broad and non-specific statutory authority to compile information and make reports to Congress conferred upon the Commission in section 6 of the FTC Act. The Commission additionally defined the application of section 5 in the Resolution by relating it to the subject matter of the investigation "the advertising, promotion, offering for sale, sale, or distribution of cigarettes...." We thus feel comfortably apprised of the purposes of the investigation and subpoenas issued in its pursuit, and suspect that respondents, who may feel less comfortable, are also quite aware of the purposes of the investigation.<sup>46</sup>

Here, the bare recitation of Section 5's "prohibition of unfair and deceptive practices ...

---

<sup>45</sup> The resolution also cannot be justified as a "blanket resolution." As the FTC Operating Manual states, blanket resolutions are only appropriate "in a limited number of instances", such as to authorize second requests in antitrust investigations. O.M. 3.3.6.7.4.3.

<sup>46</sup> *F.T.C. v. Carter*, 636 F.2d 781,788 (D.C. Cir. 1980) (emphasis added).

stands broadly alone”. Accordingly, the resolution fails to reasonably define the nature and scope of the present investigation, and is therefore both invalid and incapable of providing the necessary support for the present CID. Consequently, the present CID should be quashed.

**D. The CID Improperly Demands Documents And Testimony Concerning Matters That Are Primarily Regulated By The Department Of Health And Human Services**

The CID should also be quashed because it demands documents and information concerning data security information over which the United States Department of Health and Human Services (“HHS”) has exclusive administrative and enforcement authority. As a healthcare sector corporation, Petitioner was at all times relevant to the 2008 download of the 1,718 File regulated by HHS with respect to the privacy rules and patient data security requirements related to PHI under the Health Insurance Portability and Accountability Act (“HIPAA”).<sup>47</sup> It is undisputed that Congress gave HHS exclusive administrative and enforcement authority over data privacy and security issues.<sup>48</sup> As former FTC Chairman Deborah Majoras told Congress in 2005, HIPAA and its Privacy Rule are not enforced by the FTC.<sup>49</sup> This understanding was affirmed before Congress a year later by FTC Associate Director Joel Winston.<sup>50</sup> Accordingly, it is unreasonable and unduly burdensome to subject Petitioner to the broad investigative demands made in the present CID as the FTC is not the primary regulator of data privacy and security issues in the healthcare sector, and unlike HHS, the FTC does not have

---

<sup>47</sup> 45 C.F.R. § 160.300 *et seq.*

<sup>48</sup> *See* 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000).

<sup>49</sup> Deborah Platt Majoras, Chairman of the Federal Trade Commission, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information*, a prepared statement before the U.S. Senate, Committee on Banking, Housing, and Urban Affairs (Mar. 10, 2005).

<sup>50</sup> Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, Statement of Joel Winston, a prepared statement before the U.S. House of Representatives, Subcommittee on Social Security of the House Committee on Ways and Means (Mar. 30, 2006).

the Congressionally-delegated administrative or enforcement powers (or responsibilities) concerning these issues.

Consequently, the present CID improperly inserts the FTC into what is squarely the regulatory jurisdiction of HHS without providing any legal or policy justification for doing so. A regulated entity like Petitioner is entitled to one consistent set of data privacy and security regulations. By order of Congress, that set of regulations comes from HHS, not the FTC. Accordingly, the CID should be quashed.

### III. CONCLUSION

Because the present CID was issued pursuant to an impermissible exercise of the FTC's Section 45 authority — namely, because there is no basis in law or fact for using the 2008 download of the 1,718 File as grounds to conduct an unbounded, undefined, highly burdensome, and purposeless investigation into Petitioner's data security practices and policies, and further because such an investigation would impermissibly intrude upon the regulatory jurisdiction of a sister agency — the present CID should be quashed.

Dated: January 10, 2012



Claudia Callaway, Esq.  
Christina Grigorian, Esq.  
Julian Dayal, Esq.  
Katten Muchin Rosenman LLP  
2900 K Street, NW  
North Tower - Suite 200  
Washington, DC 20007  
Phone: (202) 625-3613  
Facsimile: (202) 298-7570  
Email: claudia.callaway@kattenlaw.com

*Counsel for Petitioner*

COMMERCIAL  
SECTION  
SECTION

**CERTIFICATION**

Pursuant to 16 C.F.R. § 2.7(d)(2), counsel for Petitioner hereby certifies that counsel met and conferred with FTC counsel in a good faith effort to resolve by agreement the issues set forth in this Petition, but the parties were unable to reach agreement.

  
\_\_\_\_\_  
Julian Dayal

### CERTIFICATE OF SERVICE

I hereby certify that on the 10th day of January, 2012, I caused the original and 12 copies of the foregoing Petition to Quash with attached exhibits to be filed by hand delivery with the Secretary of the Federal Trade Commission, 601 New Jersey Avenue, N.W., Washington, DC, 20580, and one copy of same to be filed by hand delivery with Alain Sheer, Esq., Federal Trade Commission, Division of Privacy and Identity Protection, 601 New Jersey Avenue, N.W., Washington, D.C., 20580.

  
\_\_\_\_\_  
Julian Dayal

# **EXHIBIT**

**17**



Office of the Secretary

UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, DC

April 20, 2012

**VIA E-MAIL AND COURIER DELIVERY**

Claudia Callaway, Esq.  
Christina Grigorian, Esq.  
Julian Dayal, Esq.  
Katten Muchin Rosenman LLP  
2900 K Street, N.W.  
North Tower - Suite 200  
Washington, D.C. 20007  
E-mail: claudia.callaway@kattenlaw.com

**RE:** *LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand; and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand*

Dear Ms. Callaway, Ms. Grigorian, and Mr. Dayal:

On January 10, 2012, the Federal Trade Commission ("FTC" or "Commission") received the above Petitions filed by LabMD, Inc. ("LabMD") and its President, Michael J. Daugherty (collectively, "Petitioners"). This letter advises you of the Commission's disposition of the Petitions, effected through this ruling by Commissioner Julie Brill, acting as the Commission's delegate.<sup>1</sup>

For the reasons explained below, the Petitions are denied. You may request review of this ruling by the full Commission.<sup>2</sup> Any such request must be filed with the Secretary of the Commission within three days after service of this letter ruling.<sup>3</sup> The timely filing

---

<sup>1</sup> See 16 C.F.R. § 2.7(d)(4).

<sup>2</sup> 16 C.F.R. § 2.7(f).

<sup>3</sup> *Id.* This ruling is being delivered by e-mail and courier delivery. The e-mail copy is provided as a courtesy, and the deadline by which an appeal to the full Commission

of a request for review by the full Commission shall not stay the return dates established by this ruling.<sup>4</sup>

## I. INTRODUCTION

The FTC commenced its investigation into the adequacy of LabMD's information security practices in January 2010, after a LabMD file had been discovered on a peer-to-peer ("P2P") file sharing network.<sup>5</sup> The file, which Petitioners call the "1,718 File" because it is 1,718 pages long, is a spreadsheet of health insurance billing information for uropathology and microbiology medical tests of around 9,000 patients. It contains highly sensitive information about these consumers, including:

- Name;
- Social Security Number;
- Date of birth;
- Health insurance provider and policy number; and
- Standardized medical treatment codes.<sup>6</sup>

Such information can be misused to harm consumers.

The purpose of the investigation is to determine whether Petitioners violated the FTC Act by engaging in deceptive or unfair acts or practices relating to privacy or information security. The inquiry is authorized by Resolution File No. P954807, which provides for the use of compulsory process in investigations of potential Section 5 violations involving "consumer privacy and/or data security."

---

would have to be filed should be calculated from the date on which you receive the original letter by courier delivery.

<sup>4</sup> *Id.*

<sup>5</sup> P2P programs allow users to form networks with others using the same or a compatible P2P program. Such programs allow users to locate and retrieve files of interest to them that are stored on computers of other users on the networks.

<sup>6</sup> LabMD Pet., Ex. C, at Fig. 4. Because the LabMD and Daugherty Petitions make the same arguments (the Petitions differ only in details about the submitter), we generally cite only to LabMD's Petition.

The investigation began with voluntary information requests for documents and information about LabMD's information security policies, procedures, practices, and training generally, as well as information about security incidents, including, but not limited to, the discovery of the 1,718 File on P2P networks. In response, LabMD produced hundreds of pages of documents, including supplements and responses to follow-up questions. To complete the investigation, staff requested issuance of CIDs to LabMD and Michael J. Daugherty, LabMD's President.

The Commission issued the CIDs on December 21, 2011. Both require testimony relating to information security policies, practices, training, and procedures. They also include a limited number of interrogatories that require Petitioners to identify documents used by the witnesses to prepare for their testimony.<sup>7</sup> The LabMD CID also includes a single document request asking for only those documents that were both identified in response to the CID's interrogatories and had not been previously produced to staff.<sup>8</sup>

Petitioners seek to quash or limit the CIDs because, they claim, the CIDs "appear to be premised on" the download of the 1,718 File (hereinafter, the "File disclosure").<sup>9</sup> Their principal objection relates to the merits of the investigation. In particular, they contend (without citing any authority) that the Commission must have a "justifiable" belief that a law violation has occurred before it can issue CIDs, and that the File disclosure cannot support such a belief. They claim that the File disclosure occurred not because LabMD failed to implement reasonable and appropriate security measures, but because the company was the victim of an illegal intrusion conducted by Tiversa (a P2P information technology and investigation services company) and Dartmouth College faculty using Tiversa's powerful P2P searching technology.<sup>10</sup> Further, Petitioners argue that no actual harm to consumers resulted from the File disclosure.<sup>11</sup> Accordingly, they

---

<sup>7</sup> LabMD Pet., Ex. A.

<sup>8</sup> LabMD Pet., Ex. A.

<sup>9</sup> LabMD Pet., at 1.

<sup>10</sup> Petitioners claim that in the course of a Department of Homeland Security-funded research project, Professor M. Eric Johnson of Dartmouth College's Tuck School of Business and Tiversa used Tiversa's P2P searching technology to search for and then download the file. LabMD Pet., at 3-4, 7, & Ex. F, at 10-12.

<sup>11</sup> The Petitions claim that there is no allegation of actual consumer injury from the File disclosure. LabMD Pet., at 7.

contend that investigating either the File disclosure or the adequacy of LabMD's security practices is improper because no law violation can have occurred, and that the CIDs therefore should be quashed.<sup>12</sup>

As discussed below, these arguments are undermined by: (1) the obvious point that an investigation necessarily must precede assessment of whether there is reason to believe a law violation may have occurred (in any matter); (2) the scope of the authorizing resolution; and (3) the language of the FTC Act. The resolution authorizes use of compulsory process in an investigation to determine whether Petitioners engaged in deceptive or unfair practices related to privacy or security. Petitioners' focus on the File disclosure is misplaced – it may bear on the adequacy of LabMD's security practices under the FTC Act but does not establish the investigation's scope under the resolution.<sup>13</sup> Further, in such an investigation Section 5 directs the Commission to consider whether security practices are unfair because they create a sufficient risk of harm, even if no harm has been reported.

Petitioners make two additional arguments in support of their Petitions. First, they argue that the resolution authorizing the CIDs did not provide them with sufficient notice of the purpose and scope of the investigation. Second, they argue that the FTC is without jurisdiction to pursue this investigation. Both of these additional arguments are equally without merit.

## II. ANALYSIS

### A. The applicable legal standards.

Compulsory process such as a CID is proper if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant to the inquiry, as that inquiry is defined by the investigatory resolution.<sup>14</sup>

---

<sup>12</sup> LabMD Pet., at 7-8.

<sup>13</sup> See, e.g., *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008) (confirming that the scope of an investigation authorized by Resolution P954807 properly included all of CVS' "consumer privacy and data security practices" (including its computer security practices) and could not be limited (as the company argued) to just known incidents of unauthorized disposal of paper documents in dumpsters).

<sup>14</sup> *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1088 (D.C. Cir. 1992); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977).

Agencies have wide latitude to determine what information is relevant to their law enforcement investigations and are not required to have “a justifiable belief that wrongdoing has actually occurred,” as Petitioners claim.<sup>15</sup> As the D.C. Circuit has stated, “The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudicatory one . . . . The requested material, therefore, need only be relevant to the *investigation* – the boundary of which may be defined quite generally, as it was in the Commission’s resolution here.”<sup>16</sup> Agencies thus have “extreme breadth” in conducting their investigations,<sup>17</sup> and “in light of [this] broad deference . . . , it is essentially the respondent’s burden to show that the information is irrelevant.”<sup>18</sup>

## **B. The CIDs satisfy the foregoing standards.**

Petitioners argue that the CIDs are improper for several reasons. In particular, they claim no law violation could have occurred, by arguing that: (1) not even “perfect” security measures (let alone the reasonable security measure standard the Commission uses to determine whether a law violation may have occurred) could have prevented the File disclosure because Tiversa’s technology “can penetrate even the most robust network security,”<sup>19</sup> and (2) no actual injury resulted from the File disclosure.

---

<sup>15</sup> LabMD Pet., at 6. *See, e.g., Morton Salt*, 338 U.S. at 642-43 (“[Administrative agencies have] a power of inquisition, if one chooses to call it that, which is not derived from the judicial function. It is more analogous to the Grand Jury, which does not depend on a case or controversy for power to get evidence but can investigate merely on suspicion that the law is being violated, or even just because it wants an assurance that it is not.”).

<sup>16</sup> *Invention Submission*, 965 F.2d at 1090 (emphasis in original, internal citations omitted) (citing *FTC v. Carter*, 636 F.2d 781, 787-88 (D.C. Cir. 1980), and *Texaco*, 555 F.2d at 874 & n.26).

<sup>17</sup> *Linde Thomsen Langworthy Kohn & Van Dyke, P.C. v. Resolution Trust Corp.*, 5 F.3d 1508, 1517 (D.C. Cir. 1993) (citing *Texaco*, 555 F.2d at 882).

<sup>18</sup> *Invention Submission*, 965 F.2d at 1090 (citing *Texaco*, 555 F.2d at 882) (“burden of showing that the request is unreasonable is on the subpoenaed party”). *Accord FTC v. Church & Dwight Co.*, 756 F. Supp. 2d 81, 85 (D.D.C. 2010).

<sup>19</sup> LabMD Pet., at 7.

The Commission is not required, as a precondition to conducting a law enforcement investigation, to make a showing that it is likely that a law violation has occurred. The D.C. Circuit confirmed this point in *FTC v. Texaco, Inc.*, when it stated, “[I]n the pre-complaint stage, an investigating agency is under no obligation to propound a narrowly focused theory of a possible future case . . . . The court must not lose sight of the fact that the agency is merely exercising its legitimate right to determine the facts, and that a complaint may not, and need not, ever issue.”<sup>20</sup> Here, Petitioners seek to quash the CIDs by asserting that LabMD’s practices must have been reasonable under the FTC Act because the 1,718 File was retrieved using Tiversa’s powerful searching technology. Accepting this argument would prevent the Commission from exploring relevant issues bearing on reasonableness, such as, for example, whether the company’s security practices could have prevented the 1,718 File from being retrieved using the common P2P programs that are used by millions of computer users each day or whether there were readily available security measures LabMD did not implement that would have prevented even Tiversa’s technology from successfully retrieving the file. Although such evidence (if it exists at all) could undermine their reasonableness claim, Petitioners nonetheless argue that the Commission cannot use CIDs to investigate whether the evidence exists unless it already has reason to believe it does exist. For this reason, Petitioners’ argument that the strength of Tiversa’s P2P searching technology precludes the possibility that a law violation occurred, regardless of the state of LabMD’s security, must fail.

Similarly, Petitioners’ assertion that no law violation can have occurred because no actual harm has been shown also fails because, under Section 5, a failure to implement reasonable security measures may be an unfair act or practice if the failure is *likely* to cause harm. No showing of actual harm is needed.<sup>21</sup>

Both arguments conflate the purpose of a CID with the purpose of a future potential complaint. A CID can only compel information necessary for an investigation, and the investigation may or may not result in allegations of a law violation.<sup>22</sup>

---

<sup>20</sup> 555 F.2d 862, 874 (D.C. Cir. 1977). This holding from *Texaco* has been repeatedly reaffirmed, most recently in *FTC v. Church & Dwight*, 747 F. Supp. 2d 3, 6, *aff’d*, 2011 U.S. App. LEXIS 24587 (D.C. Cir. Dec. 13, 2011).

<sup>21</sup> 15 U.S.C. § 45(n) (an unfair practice is one that “causes or *is likely to cause* substantial injury to consumers”); *see also* FTC Policy Statement on Unfairness, 104 F.T.C. 949, 1073 & n.15 (1984).

<sup>22</sup> Petitioners also argue that the CIDs are improper for other reasons. They claim that because security issues posed by P2P programs were common (according to Tiversa), such issues could not constitute an unfair or deceptive practice in violation of the FTC

Additionally, Petitioners have claimed that the CIDs are burdensome, but they have not come forward with any support for these assertions. Instead, they make only bald statements that the CIDs are “highly burdensome,” “unduly burdensome,” “costly and burdensome,” and “deeply burdensome.”<sup>23</sup> Having offered no factual information about the alleged burdens of complying with the CIDs, Petitioners have not sustained their burden to demonstrate that the CIDs are unduly burdensome.<sup>24</sup>

Such a showing would be difficult here in any event. Notwithstanding Petitioners’ description, the CIDs call primarily for testimony, not documents. Thus, it seems unlikely that compliance would require large-scale or time-consuming document production.

---

Act. LabMD Pet., at 7-8 & n.34. This argument is unavailing. The fact that a particular practice may be pervasive or widespread has no bearing on whether the FTC may investigate it as also deceptive or unfair. Indeed, accepting Petitioners’ argument would confine the FTC to investigating only those activities that were rare or uncommon, thus crippling the agency’s law enforcement mission. Along the same lines, Petitioners contend that the risks of P2P technology, and the resulting potential liabilities to businesses, were not known in 2008, when the File disclosure occurred. In support of this claim, they assert that the FTC did not notify businesses or publish guidance about P2P until 2010. LabMD Pet., at 8. In fact, many, including the FTC, warned about the risks presented by P2P programs years before the File disclosure occurred. *See, e.g.*, FTC Staff Report, “Peer-to-Peer File Sharing Technology: Consumer Protection and Competition Issues” (June 2005), available at <http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf>; Prepared Statement of the Federal Trade Commission Before The Committee on Oversight and Government Reform, United States House of Representatives (July 24, 2007) (discussing P2P programs and risks), available at <http://www.ftc.gov/os/testimony/P034517p2pshare.pdf>.

<sup>23</sup> LabMD Pet., at 7, 9, & 10.

<sup>24</sup> *See, e.g., Texaco*, 555 F.2d at 882 (“The burden of showing that the request is unreasonable is on the subpoenaed party.”) (citing *United States v. Powell*, 379 U.S. 48, 58 (1964)); *accord EEOC v. Maryland Cup Corp.*, 785 F.2d 471, 476 (4th Cir. 1986) (subpoena is enforceable absent a showing by recipient that the requests are unduly burdensome); *FTC v. Standard American, Inc.*, 306 F.2d 231, 235 (3d Cir. 1962) (recipient has responsibility to show burden and must make “a record . . . of the measure of their grievance rather than ask [the court] to assume it”); *In re Nat’l Claims Serv., Inc.*, 125 F.T.C. 1325, 1328-29 (1998) (FTC ruling that petition to quash must substantiate burden with specific factual detail).

Furthermore, to the extent that the CIDs call for narrative responses, they merely require Petitioners to identify documents related to the requested testimony. In fact, there is only one specification that requires the production of documents, and even that specification is limited to documents identified in response to the interrogatories to the extent they were “not already been produced to the FTC.”<sup>25</sup>

Finally, Petitioners, without explaining its relevance, contend that the timing of the CIDs is “troubling,” coming after LabMD’s conduct had been reviewed by two congressional committees, and after LabMD filed suit against Tiversa and others alleging conversion and trespass, among other violations, based on the File disclosure in 2008.<sup>26</sup> Though Petitioners seem to believe that there is some connection between their rejection of Tiversa’s offer to provide LabMD with information security services, their subsequent lawsuit, and the FTC’s investigation, the chronology of the investigation does not support such a conclusion. The FTC first contacted LabMD for information in January 2010, well before LabMD filed its lawsuit against Tiversa in October 2011.<sup>27</sup> Moreover, the claim that LabMD’s conduct was reviewed by congressional committees does not appear to be based on evidence presented in the Petitions. Although Petitioners have attached as exhibits three instances of congressional testimony by Tiversa, none identifies LabMD by name or discusses the specifics of the File disclosure.

**C. The resolution provides sufficient notice of the purpose and scope of the FTC’s investigation.**

Under the FTC Act, a CID is proper when it “state[s] the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation.”<sup>28</sup> It is well-established that the resolution authorizing the process provides the requisite statement of the purpose and scope of the investigation,<sup>29</sup>

---

<sup>25</sup> LabMD Pet., Ex. A.

<sup>26</sup> LabMD Pet., at 9 & Ex. F.

<sup>27</sup> We note further that this suit came more than three years after the solicitations Petitioners complain of in their Petitions. LabMD Pet., Ex. F, at 1, 17-23.

<sup>28</sup> 15 U.S.C. § 57b-1(c)(2).

<sup>29</sup> *Invention Submission.*, 965 F.2d at 1088; *accord Texaco*, 555 F.2d at 874; *FTC v. Carter*, 636 F.2d 781, 789 (D.C. Cir. 1980); *FTC v. Anderson*, 631 F.2d 741, 746 (D.C. Cir. 1979).

and also that the resolution may define the investigation generally, need not state the purpose with specificity, and need not tie it to any particular theory of violation.<sup>30</sup>

Despite this, Petitioners object that Resolution File No. P954807 did not provide sufficient notice of the purpose and scope of the investigation, and they further claim that this resolution is inadequate under the standard developed by the D.C. Circuit in *FTC v. Carter*, 636 F.2d 781, 788 (D.C. Cir. 1980).<sup>31</sup>

Petitioners' first argument reads the governing standard too narrowly. Resolution File No. P954807 authorizes the use of compulsory process:

to determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended.<sup>32</sup>

This general statement of the purpose and scope of the investigation is more than sufficient under the standard for such resolutions, and courts have enforced compulsory process issued under similarly broad resolutions.<sup>33</sup>

Petitioners' reliance on *Carter* is also misplaced. While *Carter* held that a bare reference to Section 5, without more, "would not serve very specific notice of purpose," the Court approved the resolution at issue in that case, noting that it also referred to specific statutory provisions of the Cigarette Labeling and Advertising Act, and further

---

<sup>30</sup> *Invention Submission*, 965 F.2d at 1090; *Texaco*, 555 F.2d at 874 & n.26; *FTC v. Nat'l Claims Serv., Inc.*, No. S 98-283 FCD DAD, 1999 WL 819640, at \*2 (E.D. Cal. Feb. 9, 1999) (citing *EPA v. Alyeska Pipeline Serv. Co.*, 836 F.2d 443, 477 (9th Cir. 1988)).

<sup>31</sup> LabMD Pet., at 10-12.

<sup>32</sup> LabMD Pet., Ex. A.

<sup>33</sup> See *FTC v. Nat'l Claims Serv.*, 1999 WL 819640, at \*2 (finding omnibus resolution referring to FTC Act and Fair Credit Reporting Act sufficient); *FTC v. O'Connell Assoc., Inc.*, 828 F. Supp. 165, 171 (E.D.N.Y. 1993) (enforcing CIDs issued pursuant to omnibus resolution). The Commission has repeatedly rejected similar arguments about such omnibus resolutions. See, e.g., *Firefighters Charitable Found.*, No. 102-3023, at 4 (Sept. 23, 2010); *D. R. Horton, Inc.*, Nos. 102-3050, 102-3051, at 4 (July 12, 2010); *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008).

related it to the subject matter of the investigation.<sup>34</sup> With this additional information, the Court felt “comfortably apprised of the purposes of the investigation and the subpoenas issued in its pursuit . . . .”<sup>35</sup>

The resolution here, like the one in *Carter*, does not cite solely to Section 5, but also recites the subject matter of the investigation: “deceptive or unfair acts or practices related to consumer privacy and/or data security.” Since the resolution here discloses the subject matter of the investigation in addition to invoking Section 5, the resolution provides notice sufficient under *Carter* of the purpose and scope of the investigation.

As a final note, the history of the investigation itself undermines Petitioners’ argument that the present CIDs do not sufficiently advise them of the nature and scope of the investigation. Petitioners have been under investigation since January 2010 and have engaged in repeated discussions with staff. At no point have Petitioners indicated they did not understand the purpose or scope; in fact, Petitioners have already produced hundreds of pages of documents in response to staff requests. Moreover, the Petitions under consideration here present highly detailed and factual arguments going to the very merits of the investigation. The Commission has previously found that such interactions may be considered along with the resolution in evaluating the notice provided to Petitioners.<sup>36</sup>

**D. Petitioners’ challenge to the FTC’s regulatory authority is premature and without basis.**

Petitioners’ final argument is that the FTC lacks jurisdiction to conduct the instant investigation.<sup>37</sup> Petitioners assert that LabMD is a health care company and that the

---

<sup>34</sup> *Carter*, 636 F.2d at 788.

<sup>35</sup> *Id.*

<sup>36</sup> *Assoc. First Capital Corp.*, 127 F.T.C. 910, 915 (1999) (“[T]he notice provided in the compulsory process resolutions, CIDs and other communications with Petitioner more than meets the Commission’s obligation of providing notice of the conduct and the potential statutory violations under investigation.”).

<sup>37</sup> Petitioners also claim that the resolution does not meet the requirements established by the FTC’s Operating Manual. LabMD Pet., at 10. As discussed above, by disclosing the statutory basis and subject matter of the investigation, the resolution does provide notice as required by the Operating Manual. That said, the Operating Manual, by its own terms, is advisory. It is not a “basis for nullifying any action of the Commission or the staff.”

information disclosed in the 1,718 File is protected health information (“PHI”) under the Health Insurance Portability and Accountability Act (“HIPAA”). Accordingly, they contend, the adequacy of their security practices with respect to this information is subject to the exclusive jurisdiction of HHS.<sup>38</sup>

As an initial matter, it is well-established that challenges to the FTC’s jurisdiction are not properly raised through challenges to investigatory process. As the D.C. Circuit stated: “Following *Endicott [Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943)]*, courts of appeals have consistently deferred to agency determinations of their own investigative authority, and have generally refused to entertain challenges to agency authority in proceedings to enforce compulsory process.”<sup>39</sup> The reasons for such a rule are obvious. If a party under investigation could raise substantive challenges in an enforcement proceeding, before the agency has obtained the information necessary for its case – essentially requiring the FTC to litigate an issue before it can learn about it – then the FTC’s investigations would be foreclosed or substantially delayed.<sup>40</sup> Thus, Petitioners’ basic challenge to the FTC’s jurisdiction is premature and will not support quashing the instant CIDs.

In any event, the claim that HHS has exclusive jurisdiction to investigate privacy and data security issues involving PHI is without basis. Petitioners essentially invoke the doctrine of implied repeal to assert that HIPAA and its Privacy and Security Rules displace FTC jurisdiction. But implied repeal is “strongly disfavored,” for two reasons.<sup>41</sup> First, courts have recognized that agencies may have overlapping or concurrent jurisdiction, and thus that the same issues may be addressed and the same parties

---

Operating Manual, § 1.1.1.1. *See also FTC v. Nat’l Bus. Consultants, Inc.* 1990 U.S. Dist. LEXIS 3105, 1990-1 Trade Cas. (CCH) ¶68,984, at \*29 (E.D. La. March 19, 1990).

<sup>38</sup> LabMD Pet., at 12-13.

<sup>39</sup> *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001) (citing *United States v. Sturm, Ruger & Co.*, 84 F.3d 1, 5 (1st Cir. 1996)); *United States v. Construction Prods. Research, Inc.*, 73 F.3d 464, 468-73 (2d Cir. 1996); *EEOC v. Peat, Marwick, Mitchell & Co.*, 775 F.2d 928, 930 (8th Cir. 1985); *Donovan v. Shaw*, 668 F.2d 985, 989 (8th Cir. 1982); *FTC v. Ernstthal*, 607 F.2d 488, 490 (D.C. Cir. 1979); accord *Oklahoma Press Publ’g Co. v. Walling*, 327 U.S. 186, 213-14 (1946).

<sup>40</sup> *Texaco*, 555 F.2d at 879.

<sup>41</sup> *Galliano v. United States Postal Serv.*, 836 F.2d 1362, 1369 (D.C. Cir. 1988).

proceeded against simultaneously by more than one agency.<sup>42</sup> Second, courts rarely hold that one federal statute impliedly repeals another because ““when two statutes are capable of co-existence, it is the duty of the courts . . . to regard each as effective.””<sup>43</sup> Thus, repeals by implication will only be found where the Congressional intent to effect such a repeal is “clear and manifest.”<sup>44</sup>

Petitioners can point to no such “clear or manifest” evidence that Congress intended HIPAA or its rules to displace the FTC Act. The authority Petitioners cite for the proposition that HHS has exclusive jurisdiction does not address such repeal.<sup>45</sup> To the contrary, there is ample evidence against such implied repeal. For one, the same authority cited by Petitioners – the preamble to the Privacy Rule – expressly provides that entities covered by that Rule are “also subject to other federal statutes and regulations.”<sup>46</sup> Also, this preamble includes an “Implied Repeal Analysis,” which is silent as to any implied repeal of the FTC Act.<sup>47</sup> Recent legislation shows that, if anything, Congress intended the FTC and HHS to work collaboratively to address potential privacy and data security risks related to health information. The American Recovery and Reinvestment Act of 2009, for instance, required HHS and the FTC to develop harmonized rules for data breach notifications by HIPAA-covered and non-HIPAA-covered entities, respectively. *See* 74

---

<sup>42</sup> *FTC v. Cement Inst.*, 333 U.S. 683, 694 (1948); *see also Texaco*, 555 F.2d at 881 (“[T]his is an era of overlapping agency jurisdiction under different statutory mandates.”); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1986). Because agencies have overlapping jurisdiction, they often work together. For instance, the FTC and HHS collaborated on the investigation of CVS Caremark Corporation. *See CVS Caremark Corp.*, No. 072-3119, at 7 (Aug. 6, 2008).

<sup>43</sup> *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 155 (1976) (quoting *Morton v. Mancari*, 417 U.S. 535, 551 (1974)).

<sup>44</sup> *Id.* at 154.

<sup>45</sup> LabMD Pet., at 12 (citing 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000)). This Federal Register notice is the Notice of Public Rulemaking for the Privacy and Security Rules under HIPAA. The excerpt cited by Petitioners does not address the scope of HHS’ enforcement jurisdiction, but rather discusses the delegation of enforcement authority from the Secretary of HHS to HHS’ Office for Civil Rights. 65 Fed. Reg. 82,472 (Dec. 28, 2000).

<sup>46</sup> 65 Fed. Reg. 82,462, 82,481 (Dec. 28, 2000).

<sup>47</sup> *Id.* at 82,481-487.

Fed. Reg. 42,962, 42,962-63 (Aug. 25, 2009). Thus, HIPAA and its Rules do not serve to repeal FTC jurisdiction, which is overlapping and concurrent to HHS’.

This is particularly appropriate where, as here, the consumer information at issue included more than just health information. The consumer information exposed in the 1,718 File also included names, Social Security numbers, and dates of birth. While this information can be considered PHI under HIPAA when combined with health information, the information clearly exposes consumers to the risk of identity theft and is exactly the kind of sensitive personal information that the Commission is charged with protecting under Section 5 of the FTC Act and other statutes. Petitioners have provided no proper basis to challenge the investigation as an exercise of the Commission’s jurisdiction under these authorities.

### III. CONCLUSION AND ORDER

For the foregoing reasons, **IT IS HEREBY ORDERED THAT** LabMD, Inc.’s Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

**IT IS FURTHER ORDERED THAT** Michael J. Daugherty’s Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

**IT IS FURTHER ORDERED THAT** Commission staff may reschedule the investigational hearings of LabMD and Michael J. Daugherty at such dates and times as they may direct in writing, in accordance with the powers delegated to them by 16 C.F.R. § 2.9(b)(6); and

**IT IS FURTHER ORDERED THAT** all other responses to the specifications in the Civil Investigative Demands to LabMD, Inc. and Michael J. Daugherty must now be produced on or before May 11, 2012.

By direction of the Commission.

Donald S. Clark  
Secretary

# **EXHIBIT**

**18**