

HOUSE OVERSIGHT AND GOVERNMENT REFORM

THURSDAY, JULY 24, 2014

The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury

Written Testimony

Michael J. Daugherty

CEO, LabMD, Inc.

Good Morning Mr. Chairman and members of the Committee. My name is Michael Daugherty. I am the President and CEO of LabMD, Inc., a cancer detection laboratory based in Atlanta, Georgia. We were a private company that I founded in 1996. A small medical facility that at its peak employed approximately forty (40) medical professionals who touched nearly one million American lives. Thank you for the opportunity to speak to you today about my experience at the hands of the Federal Trade Commission and its advisor, Tiversa.

This story transcends party politics and touches all Americans. What happened to my company, its employees, and the physicians and their patients that we served is emblematic of what can result from the FTC's unsupervised administrative playbook. That playbook relies upon coercive and extortionate strategies to make small and large companies alike quickly succumb to FTC demands. The FTC's reliance upon unverified allegations as "evidence" is an embarrassment to the agency. Moreover, its association with a company that extorts funds from American businesses is reprehensible and violative of the "pact" between citizens and their government. With the FTC, you aren't just guilty until proven innocent, you're guilty because the FTC says so...and dead before they're done.

Set forth below is a timeline recounting the six year battle that LabMD has fought. Six years of attorneys' fees. Six years of unfounded accusations. And, finally, after a costly battle and extensive carnage, the hope provided when this Committee announced its investigation.

May 2008

My nightmare began with a call that could happen to any American. It was from Robert Boback, the CEO of Tiversa. In the words of one FTC Commissioner, "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." Mr. Boback told me that Tiversa had found LabMD patient data on the Internet, but refused to tell us more **unless we paid and retained them.**

In response to Tiversa's call, we performed a security review and determined that no patient files had been disseminated. Frankly, we were appalled by Tiversa's "protection racket" tactic: Everyone in medicine knows you can't go out intentionally looking for vulnerable medical files, take them, read them, keep them and distribute them. Tiversa's "hire us or else" threats were outrageous. But as you will see from my testimony, these threats foreshadowed the actions that would lead to the demise of LabMD and the forty (40) full-time jobs it had created in its aim to support medical professionals in their assessment of cancer indicators.

Tiversa continued trying to scare us by asking, for example, if we had seen the story in the Washington Post that Supreme Court Justice Breyer had his files taken. Tiversa wanted us to pay them approximately \$40,000 to remedy the so-called “breach.” We told them that we suspected Tiversa itself of wrongdoing, and asked that they no longer contact us.

November 2008

Tiversa called again -- this time, aggressive, accusatory, and defensive. He said that Tiversa was giving the LabMD files to the FTC. We went back to diagnosing cancer with one eye over our shoulder, and continued to look for our patient data on the Internet. We never found it – there was simply no distribution of LabMD data that could be verified or substantiated. Because the file was not “out there”, we assumed that the FTC would recognize the game that Tiversa was playing, and give no additional thought to Tiversa’s allegations against us. No other course of action would make sense.

January 2010

Alain Sheer, an attorney with the FTC, contacted LabMD with an 11 page, single spaced letter opening a “nonpublic inquiry”. We responded by inviting the FTC to come to Atlanta – to see our facility; to tell us what we were to do differently; **to tell us just what the standards are.** The FTC declined. We quickly discovered that until told otherwise by the courts or Congress, the FTC presumes to have jurisdiction to investigate any company or person.

August 2010

It became clear that I would have to come to my own rescue so I started my own research. What I discovered was Kafkaesque:

Tiversa's Robert Boback appeared before this Committee in 2009 and made good on his threat to us. Without regard to federal privacy laws, or the dignity of cancer patients, Tiversa had disseminated LabMD's unredacted patient files to Dartmouth College, who then used the data in its study on "Data Hemorrhages in the Medical Space." Tiversa then provided a redacted form of these files to both Wired Magazine and to this Committee.

Digging deeper, I learned that the Tiversa-Dartmouth connection was this: the Department of Homeland Security gave \$24 million to Dartmouth to partially fund the "Data Hemorrhage" study. Dartmouth states that it got the file for this study using Tiversa's unique and powerful technology. Tiversa was so proud of this they put out a press release in May of 2009 which in part stated:

"Tiversa today announced the findings of new research that revealed 13,185,252 breached files emanating from over 4,310,839 sources.... Tiversa's patent pending technology monitors roughly 450 million users issuing 1.5 billion searches a day....Over a two-week period, Dartmouth College researchers and Tiversa searched file-sharing networks...and discovered a treasure trove...a spreadsheet from an AIDS clinic with 232 client names, SS#'s addresses and birth dates...a 1718 page document from a medical testing laboratory. Requiring no software or hardware, Tiversa detects, locates and identifies exposed files in real-time..."

We now know that this is not true. We learned that Tiversa did NOT get this file as portrayed in the Dartmouth study and Tiversa and Dartmouth knew it. Dartmouth got LabMD's files when Dartmouth said – and I quote – they wanted to "spice up the data",

and Tiversa provided them with the file. So Tiversa – which had expressed its deepest concern to us in May of 2008 regarding the security of these files – was now distributing LabMD property without regard to my company's patients, and still would not answer our questions about how the property was acquired.

August 2011

After twenty (20) months, hundreds of thousands of dollars in lawyer fees, and technology upgrades to a standard that we could only guess at, I asked the FTC if they needed ANYTHING ELSE from us. Their answer was no. Soon after, Alain Sheer and Ruth Yodaikan told us they wanted LabMD to enter into a consent decree. I told them no, as the FTC had not pointed to any wrongdoing by LabMD, and we could not consent to something that was not true. They said they would sue the next day. But no suit was filed – yet.

December 2011

Instead of filing a lawsuit against LabMD – and perhaps in recognition that they could not articulate any wrong doing by LabMD – the FTC instead served a Civil Investigative Demand – essentially, an administrative subpoena – upon me, commanding that I sit for a deposition. Based upon my conversation with the FTC in August of 2011 that they did not need more information, I filed a formal objection to the CID. Unbelievably, the FTC's rules precluded me from attending the hearing regarding this motion. The motion was denied.

We appealed the decision to the Commission, setting forth Tiversa's creation of the FTC's investigation after LabMD refused to retain Tiversa. While our appeal was denied, FTC Commissioner Rosch registered his dissent from the majority, and expressed concern about Tiversa's involvement, noting that Tiversa had a commercial interest in the outcome of the investigation, and questioning its business model.

August 2012

The FTC filed suit in Federal Court to make us sit for more depositions. The Court ruled that the FTC can haul in pretty much anyone they want.

February 2013

These depositions – in which the FTC asked the same questions over and over in an effort to deplete our financial resources so that we would not be able to afford an appeal to federal court – wore down the LabMD staff and emptied our bank accounts. Finally, the FTC alleged that it had discovered a “hard copy” of a spreadsheet of information concerning 500 LabMD patients in Sacramento, California. The FTC couldn't prove where it came from, and sat on the information for months without telling us they had it (thereby themselves violating HIPAA time notification regulations). None of this made any sense.

August 28, 2013

The Associated Press woke me up with a phone call telling me that I had been sued by FTC. The public relations arm of the FTC had issued a scathing press release at the same time they filed suit.

September 2013 – April 2014

The FTC pursued litigation against LabMD via their optional administrative process rather than in the Federal courts. This administrative adjudication vehicle was identified by FTC Commissioner Wright last December as providing the FTC with “[I]nstitutional and procedural advantages” over its targets. As I learned, a target gets drained dry financially in a forum where a judge who doesn’t agree with the FTC gets overturned by the Commissioners. So what is the point? The point is to exhaust your insurance, your lawyers, and your fortitude before you can get out of there. And federal courts won’t intervene because they say Congress says they can’t.

When asked by the administrative law judge about the FTC Data Security standards, Alain Sheer – one of approximately twenty (20) lawyers representing the FTC in the matter – said, and I quote, “There is nothing out there for a company to look at....there is no rulemaking...no rules have been issued.” Yet even without any standards, they subpoenaed approximately forty (40) different individuals: long-gone LabMD employees that left the company up to 7 years ago, current LabMD staff, managers, physicians, vendors. These witnesses were forced to retain counsel, and the FTC seemed to say:

“This is FTC Justice and what will happen to you if you don’t play along, so cooperate please.”

January 15, 2014

As a result of the strain and expense of nearly five years of litigation with the FTC – litigation for which no legal standard was ever articulated – LabMD ceased its operations. Everyone lost their job, and doctors scrambled for a new lab. The FTC tore the soul out of LabMD.

May 2014

The trial started in Administrative Court the FTC’s headquarters. The FTC called four “expert” witnesses, all of whom were told to assume that LabMD had flawed data security practices, and to rely upon Tiversa’s unproven representations that the LabMD file had been “spread.”

June 2014

A former Tiversa employee who was to testify at trial regarding Tiversa’s acquisition of LabMD data and subsequent submission of the data to the FTC invoked his Fifth Amendment right against self-incrimination. This Committee announced its investigation, and the trial case was stayed.

* * *

All Americans should be outraged by the FTC's unchecked ability to pursue a claim that is not based in any legal standard. Outraged that the FTC's administrative proceedings do not afford the same guarantees of due process that our federal courts provide. And outraged with the FTC's use of and reliance upon information from a private, for-profit entity that made good on its threat to destroy a small medical lab. Because if it could happen to LabMD, it could happen to anyone. (And, indeed, it did happen to Chicago's Open Door Clinic and others.)

As a reminder, LabMD was a small cancer detection lab, working to create jobs in a difficult economy. LabMD was shuttered because it refused to cave – first to Tiversa and then, as threatened, to the FTC's unfair process. Being accused of mishandling medical files is fatal to a cancer detection lab. The fact that the FTC made this accusation so casually and recklessly was astounding. We had built a company based upon the most precious commodities available – trust and integrity – and the FTC had destroyed it based upon nothing more than an unverified accusation by a self-interested commercial suitor whom we had scorned.

This Committee has the power to get answers to the questions that LabMD posed, but for which we were never provided a response: How, really, did Tiversa obtain LabMD files? When did Tiversa meet with the FTC and agree to provide the FTC with those files? How was Tiversa compensated for providing this information? What did the FTC know about Tiversa's creation of "The Privacy Institute," which Mr. Boback testified was

formed for the sole purpose of transmit information to the FTC while “provid[ing] some separation from Tiversa from getting a civil investigative demand”? By getting answers to these questions, this Committee’s work will help all Americans, and will ensure the fair governmental system envisioned by our nation’s founders.

I thank the Committee for its time and attention to this matter.



October 5, 2010

Tiversa
Attn: Mr. Robert Boback
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066

RE: LabMD, Inc.

Dear Mr. Boback:

I am conducting an investigation on behalf of LabMD. I am investigating the abuse and misappropriation of LabMD's property that may have involved any number of legal infractions, possibly including but not limited to, theft, conversion, extortion, trespass, privacy infringement, copyright infringement, computer crime, and misappropriation of trade secrets.

We have become aware that a certain pdf file containing insurance aging information has come into the possession of you, Dartmouth University and the United States Federal Trade Commission ("FTC"). Our investigation has not determined how this property came into your possession. LabMD has not authorized or granted permission to anyone to take possession of this property or to use, process, or change it in any way.

For example, we see a redacted version of LabMD's property published in the following *Wired Magazine* article, "Academic Claims to Find Sensitive Medical Info Exposed on Peer-to-Peer Networks" <<http://www.wired.com/threatlevel/2009/03/p2p-networks-le/>>. Mr. Alain Sheer and you have both informed LabMD that they possess this property. More than one news article has referenced this property in a way suggesting that it is in the possession of Professor Eric Johnson and Dartmouth University. At this stage of the investigation, we have many unanswered questions. We ask that you cooperate with our investigation in answering the following questions:

DEFINITIONS

Accordingly, as used herein, the terms "you" or "your" refers, without limitations, to the recipients of this letter, their representatives, agents, and all persons acting in their behalf.

As used herein, the term "record" shall mean any electronic, written, recorded, or graphic matter, whether produced, reproduced or stored electronically, on papers, cards, tapes, belts, or computer devices of any other medium in possession, custody or control or known by you to exist and includes originals, all copies of originals, and all prior drafts. When the term "identify," is used in conjunction with the term "record," you are to state, with respect to such record: (1) the date of the record; (2) the identity of the person who has custody or control over the record; and (3) the nature and substance of the record, all with sufficient particularity to enable it to be identified in a notice to produce.

"Identify," with respect to a person, firm, corporation or other entity, means to provide an exact name, place of business, address, and telephone number.

"Identify," with respect to any record, means to provide the title and date of such record, the identity of the person preparing it, the identity of the custodian of the record, a description of the type of record (e.g., electronic data file, photograph, report, summary, etc.), database filename, and a description of what each record contains, depicts, reveals, or says.

As used herein, the term "date" shall mean the exact day, month, and year if ascertainable, or, if not, the best approximation including relationship to other events.

INVESTIGATIVE QUESTIONS

1. What method, manner, services, technologies, and/or parties were utilized to access and obtain possession of LabMD's property?
2. Have you shared LabMD's property with anyone, whether redacted or not? If so, with whom and under what circumstances?
3. Do you have a financial or business relationship with Dartmouth College or the United States Federal Trade Commission ("FTC") that would be relevant to LabMD's property and/or your access and/or possession of LabMD's property?
4. To your knowledge, what are and have been the financial, business, or other relationships between you and/or Dartmouth College and/or the FTC?
5. Please identify all records and data you possess that belong to LabMD or pertain to LabMD.
6. Please identify any and all records and data belonging or pertaining to LabMD that you have accessed or reviewed, whether currently in your possession or not.

- 7. Please identify and disclose the identity of any and all communications you have had with Dartmouth College, the FTC or any other individual or party regarding LabMD or its property.**
- 8. If you have engaged in communications with anyone regarding LabMD or its property, whether specifically naming LabMD or not, please state the purpose and content of any such communications.**
- 9. Please provide the dates and form of any communications listed in response to items numbered 7 & 8 above.**
- 10. What was your justification for accessing, taking possession, processing, storing and/or examining LabMD's property?**
- 11. Please provide a full explanation of how you examined, interrogated, changed, processed, stored and/or transmitted LabMD's property.**
- 12. What was your justification for opening any file that is LabMD's property?**
- 13. Please provide a full explanation of the security that you have and are now applying to any and all property belonging to LabMD.**
- 14. Please provide a full explanation, if you have destroyed any records, related to your acquisition, processing, or possession of LabMD's property or records.**
- 15. If you have destroyed any such records referenced in item no. 14 above, please identify each record and the date each record was destroyed.**
- 16. Were you involved in (or have you witnessed on the part of any other recipients to this letter) a pattern of conduct, involving taking property like LabMD's property in connection with attempts to solicit the property owners as clients, threats to expose the property to authorities, and/or efforts to reap benefits from the property.**

Please be advised that you should take the necessary steps to preserve and safeguard any LabMD property in your possession, and any and all records related to your possession of LabMD's property, included but not limited to, electronic mail, metadata, and IT logs.

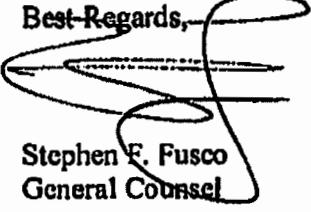
LabMD intends to take all appropriate steps to protect its rights and to protect the integrity and security of the data contained in its property.

LabMD takes a very dim view of this abuse of its property. This is a serious investigation that may involve many stages. We ask that you provide complete answers

Tiversa
October 5, 2010
Page 4 of 4

to the foregoing investigative questions within thirty (30) days of your receipt of this letter.

Thank you in advance for your cooperation with this investigation.

Best Regards,

Stephen F. Fusco
General Counsel

cc: Philippa V. Ellis, Esq.



October 5, 2010

Dartmouth College
Office of the General Counsel
Attn.: Robert B. Donin, Esq.
14 South Main Street, Suite 2C
Hanover, New Hampshire 03755

RE: LabMD, Inc.

Dear Robert:

I am conducting an investigation on behalf of LabMD. I am investigating the abuse and misappropriation of LabMD's property that may have involved any number of legal infractions, possibly including but not limited to, theft, conversion, extortion, trespass, privacy infringement, copyright infringement, computer crime, and misappropriation of trade secrets.

We have become aware that a certain pdf file containing insurance aging information has come into the possession of Dr. M. Eric Johnson, Tiversa and the United States Federal Trade Commission ("FTC"). Our investigation has not determined how this property came into their possession. LabMD has not authorized or granted permission to anyone to take possession of this property or to use, process, or change it in any way.

For example, we see a redacted version of LabMD's property published in the following *Wired Magazine* article, "Academic Claims to Find Sensitive Medical Info Exposed on Peer-to-Peer Networks" (<http://www.wired.com/threatlevel/2009/03/p2p-networks-leak/>). Mr. Alain Sheer and Tiversa have both informed LabMD that they possess this property. More than one news article has referenced this property in a way suggesting that it is in the possession of Professor Eric Johnson and Tiversa. At this stage of the investigation, we have many unanswered questions. We ask that you cooperate with our investigation in answering the following questions:

DEFINITIONS

Accordingly, as used herein, the terms "you" or "your" refers, without limitations, to the recipients of this letter, their representatives, agents, and all persons acting in their behalf.

As used herein, the term "record" shall mean any electronic, written, recorded, or graphic matter, whether produced, reproduced or stored electronically, on papers, cards, tapes, belts, or computer devices of any other medium in possession, custody or control or known by you to exist and includes originals, all copies of originals, and all prior drafts. When the term "identify," is used in conjunction with the term "record," you are to state, with respect to such record: (1) the date of the record; (2) the identity of the person who has custody or control over the record; and (3) the nature and substance of the record, all with sufficient particularity to enable it to be identified in a notice to produce.

"Identify," with respect to a person, firm, corporation or other entity, means to provide an exact name, place of business, address, and telephone number.

"Identify," with respect to any record, means to provide the title and date of such record, the identity of the person preparing it, the identity of the custodian of the record, a description of the type of record (e.g., electronic data file, photograph, report, summary, etc.), database filename, and a description of what each record contains, depicts, reveals, or says.

As used herein, the term "date" shall mean the exact day, month, and year if ascertainable, or, if not, the best approximation including relationship to other events.

INVESTIGATIVE QUESTIONS

1. What method, manner, services, technologies, and/or parties were utilized to access and obtain possession of LabMD's property?
2. Have you shared LabMD's property with anyone, whether redacted or not? If so, with whom and under what circumstances?
3. Do you have a financial or business relationship with Tiversa or the FTC that would be relevant to LabMD's property and/or your access and/or possession of LabMD's property?
4. To your knowledge, what are and have been the financial, business, or other relationships between you and/or Tiversa and/or the FTC?
5. Please identify all records and data you possess that belong to LabMD or pertain to LabMD.
6. Please identify any and all records and data belonging or pertaining to LabMD that you have accessed or reviewed, whether currently in your possession or not.

7. Please identify and disclose the identity of any and all communications you have had with Tiversa, the FTC or any other individual or party regarding LabMD or its property.
8. If you have engaged in communications with anyone regarding LabMD or its property, whether specifically naming LabMD or not, please state the purpose and content of any such communications.
9. Please provide the dates and form of any communications listed in response to items numbered 7 & 8 above.
10. What was your justification for accessing, taking possession, processing, storing and/or examining LabMD's property?
11. Please provide a full explanation of how you examined, interrogated, changed, processed, stored and/or transmitted LabMD's property.
12. What was your justification for opening any file that is LabMD's property?
13. Please provide a full explanation of the security that you have and are now applying to any and all property belonging to LabMD.
14. Please provide a full explanation, if you have destroyed any records, related to your acquisition, processing, or possession of LabMD's property or records.
15. If you have destroyed any such records referenced in item no. 14 above, please identify each record and the date each record was destroyed.
16. Were you involved in (or have you witnessed on the part of any other recipients to this letter) a pattern of conduct, involving taking property like LabMD's property in connection with attempts to solicit the property owners as clients, threats to expose the property to authorities, and/or efforts to reap benefits from the property.

Please be advised that you should take the necessary steps to preserve and safeguard any LabMD property in your possession, and any and all records related to your possession of LabMD's property, included but not limited to, electronic mail, metadata, and IT logs.

LabMD intends to take all appropriate steps to protect its rights and to protect the integrity and security of the data contained in its property.

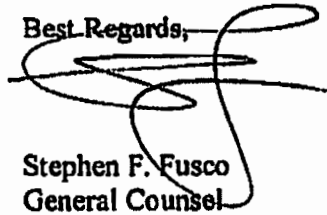
LabMD takes a very dim view of this abuse of its property. This is a serious investigation that may involve many stages. We ask that you provide complete answers

Dartmouth College
October 5, 2010
Page 4 of 4

to the foregoing investigative questions within thirty (30) days of your receipt of this letter.

Thank you in advance for your cooperation with this investigation.

Best Regards,

A handwritten signature in black ink, consisting of several loops and a long horizontal stroke, positioned over the printed name and title.

Stephen F. Fusco
General Counsel

cc: Philippa V. Ellis, Esq.



October 5, 2010

Dr. M. Eric Johnson
Tuck School of Business
Dartmouth College
100 Tuck Hall
Mail Box No. 9000
Hanover, New Hampshire 03755

RE: LabMD, Inc.

Dear Dr. Johnson:

I am conducting an investigation on behalf of LabMD. I am investigating the abuse and misappropriation of LabMD's property that may have involved any number of legal infractions, possibly including but not limited to, theft, conversion, extortion, trespass, privacy infringement, copyright infringement, computer crime, and misappropriation of trade secrets.

We have become aware that a certain pdf file containing insurance aging information has come into the possession of you, Tiversa and the United States Federal Trade Commission ("FTC"). Our investigation has not determined how this property came into your possession. LabMD has not authorized or granted permission to anyone to take possession of this property or to use, process, or change it in any way.

For example, we see a redacted version of LabMD's property published in the following *Wired Magazine* article, "Academic Claims to Find Sensitive Medical Info Exposed on Peer-to-Peer Networks" <<http://www.wired.com/threatlevel/2009/03/p2p-networks-le/>>. Mr. Alain Sheer and Tiversa have both informed LabMD that they possess this property. More than one news article has referenced this property in a way suggesting that it is in your possession and Tiversa's possession. At this stage of the investigation, we have many unanswered questions. We ask that you cooperate with our investigation in answering the following questions:

DEFINITIONS

Accordingly, as used herein, the terms "you" or "your" refers, without limitations, to the recipients of this letter, their representatives, agents, and all persons acting in their behalf.

As used herein, the term "record" shall mean any electronic, written, recorded, or graphic matter, whether produced, reproduced or stored electronically, on papers, cards, tapes, belts, or computer devices of any other medium in possession, custody or control or known by you to exist and includes originals, all copies of originals, and all prior drafts. When the term "identify," is used in conjunction with the term "record," you are to state, with respect to such record: (1) the date of the record; (2) the identity of the person who has custody or control over the record; and (3) the nature and substance of the record, all with sufficient particularity to enable it to be identified in a notice to produce.

"Identify," with respect to a person, firm, corporation or other entity, means to provide an exact name, place of business, address, and telephone number.

"Identify," with respect to any record, means to provide the title and date of such record, the identity of the person preparing it, the identity of the custodian of the record, a description of the type of record (e.g., electronic data file, photograph, report, summary, etc.), database filename, and a description of what each record contains, depicts, reveals, or says.

As used herein, the term "date" shall mean the exact day, month, and year if ascertainable, or, if not, the best approximation including relationship to other events.

INVESTIGATIVE QUESTIONS

1. What method, manner, services, technologies, and/or parties were utilized to access and obtain possession of LabMD's property?
2. Have you shared LabMD's property with anyone, whether redacted or not? If so, with whom and under what circumstances?
3. Do you have a financial or business relationship with Dartmouth College or the FTC that would be relevant to LabMD's property and/or your access and/or possession of LabMD's property?
4. To your knowledge, what are and have been the financial, business, or other relationships between you and/or Dartmouth College and/or the FTC?
5. Please identify all records and data you possess that belong to LabMD or pertain to LabMD.
6. Please identify any and all records and data belonging or pertaining to LabMD that you have accessed or reviewed, whether currently in your possession or not.

7. Please identify and disclose the identity of any and all communications you have had with Dartmouth College, the FTC or any other individual or party regarding LabMD or its property.
8. If you have engaged in communications with anyone regarding LabMD or its property, whether specifically naming LabMD or not, please state the purpose and content of any such communications.
9. Please provide the dates and form of any communications listed in response to items numbered 7 & 8 above.
10. What was your justification for accessing, taking possession, processing, storing and/or examining LabMD's property?
11. Please provide a full explanation of how you examined, interrogated, changed, processed, stored and/or transmitted LabMD's property.
12. What was your justification for opening any file that is LabMD's property?
13. Please provide a full explanation of the security that you have and are now applying to any and all property belonging to LabMD.
14. Please provide a full explanation, if you have destroyed any records, related to your acquisition, processing, or possession of LabMD's property or records.
15. If you have destroyed any such records referenced in item no. 14 above, please identify each record and the date each record was destroyed.
16. Were you involved in (or have you witnessed on the part of any other recipients to this letter) a pattern of conduct, involving taking property like LabMD's property in connection with attempts to solicit the property owners as clients, threats to expose the property to authorities, and/or efforts to reap benefits from the property.

Please be advised that you should take the necessary steps to preserve and safeguard any LabMD property in your possession, and any and all records related to your possession of LabMD's property, included but not limited to, electronic mail, metadata, and IT logs.

LabMD intends to take all appropriate steps to protect its rights and to protect the integrity and security of the data contained in its property.

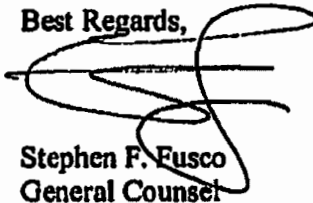
LabMD takes a very dim view of this abuse of its property. This is a serious investigation that may involve many stages. We ask that you provide complete answers

Dr. M. Eric Johnson
October 5, 2010
Page 4 of 4

to the foregoing investigative questions within thirty (30) days of your receipt of this letter.

Thank you in advance for your cooperation with this investigation.

Best Regards,

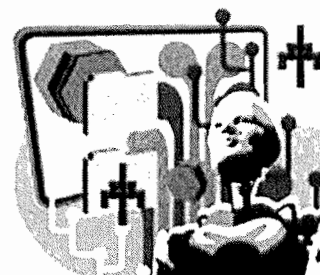
A handwritten signature in black ink, appearing to be "S. Fusco", written over a horizontal line.

Stephen F. Fusco
General Counsel

cc: Philippa V. Ellis, Esq.

theguardian

TECHNOLOGY



Dissent in the ranks: why one FTC commissioner didn't like Google's fine

The \$22.5m fine handed out to Google over its cookie-tracking of Apple users didn't satisfy one of the five Federal Trade Commissioners. But why not?



Google's cookie-tracking of Apple users attracted a fine - but was that enough? Photograph: Roger Tooth for the Guardian

One point that got mostly overlooked in the Federal Trade Commission (FTC) fine against Google - \$22.5m, which would be a lot for you or me, but amounts to about 15 hours' operating profits based on the company's operating profits from its second quarter - was the dissenting opinion of one of the five commissioners, J Thomas Rosch, from the majority.

(**Update:** Rosch has again dissented after the FTC settled with Facebook over its altering of privacy settings. More in the piece below.)

The commissioners split 4-1 in what they thought should be the correct way to treat Google over its behaviour. In fact, Rosch's dissent was so strong that the other four had to write an opinion (PDF) explaining their reasoning.

But first, here's Rosch's beef. In his minority opinion (PDF), he says that he thinks that the FTC Act obliges him (and the others)

to determine whether there is both 'reason to believe' there is liability and whether the complaint is in the 'public interest' before we vote out any complaint, whether it be a litigation complaint or a consent decree.

Clear enough so far? He's setting out what the ground rules are for deciding whether to vote on something: liability and public interest.

Now it gets interesting.

There is no question in my mind that there is "reason to believe" that Google is in contempt of a prior Commission order. However, I dissent from accepting this consent decree because it arguably cannot be concluded that the consent decree is in the public interest when it contains a denial of liability.

That is: if Google won't agree that it is liable for what it has done, then Rosch doesn't think it should be let off with just a fine. In fact, he's really quite vexed (reading between the lines) at the fact that all Google does accept about the FTC is that it has jurisdiction, and that it's doing this in the right location: He points to the FTC Order (handing down the fine) which says "[The] Defendant [Google] denies any violation of the FTC Order, any and all liability for the claims set forth in the Complaint, and all material allegations of the Complaint save for those regarding jurisdiction and venue."

Yet, at the very same time, the Commission supports a civil penalty of \$22.5 million against Google for that very same conduct. Condoning a denial of liability in circumstances such as these is unprecedented.

He also points out that Google has been charged before with "engaging in deceptive conduct" over Buzz, its social network which enrolled you whether or not you really wanted to be enrolled (much the same as Google+, in fact, though that seems to handle privacy rather better - so much better that nobody can tell how much of anything actually goes on there). Google, says Rosch, is essentially being charged with contempt of

the FTC's Consent Order over Buzz - which is how it got into this whole thing.

Says Rosch:

"This scenario – violation of a consent order – makes the Commission's acceptance of Google's denial of liability all the more inexplicable."

He points out that \$22.5m "represents a de minimis amount of Google's profit or revenues." But it's even worse, he says:

"the Commission now has allowed liability to be denied not only in this matter but also in the Facebook settlement where Facebook simply promised to 'go and sin no more' (unlike Google, Facebook was not previously under order). There is nothing to prevent future respondents with fewer resources than Google and with lower profiles than Google and Facebook from denying liability in the future too."

And that's the real nub of Rosch's complaint with the majority decision: that if you let Google (and Facebook, which was also put under a consent order essentially for swapping around its privacy rules so often) off without admitting that what they did was wrong, then others will too. And if you *don't* do that, then it becomes one law for the big guys with hefty lobbying operations, and one law for the small ones.

For complete clarity, I emailed the FTC on Thursday, and Commissioner Rosch's office responded to my queries as follows:

Commissioner Rosch doesn't think that the Commission has any business accepting a denial of liability when 1) Google sees fit to pay over \$22 million in civil penalties; 2) Google is in clear contempt of a Commission order; and 3) there is no limiting principle, so that the acceptance of a denial of liability in this case represents a precedent for respondents less well-heeled and with a lower profile than Google to also negotiate a denial of liability. Commissioner Rosch notes that the FTC has a precedent here -- it is to allow defendants to "neither admit nor deny" liability. The Commission just didn't hold Google to that precedent in this case.

Update: in his Facebook dissenting opinion (PDF), Rosch says: "I cannot find that either the "reason to believe" or the "in the interest of the public" requirement is satisfied when, as here, there is an express denial of the allegations set forth in the complaint." So it's just as with Google: Rosch feels that companies should take responsibility for their actions (or inactions) - and wants the FTC to shift to a model like

the Securities and Exchange Commission, where if you deny the charges then you can't be part of a consent order (essentially, getting you out of going to trial).

There's certainly evidence that within the FTC, Google isn't exactly flavour of the month. In a call with reporters, David Vladeck, the director of the FTC's bureau of consumer protection, pointed to other privacy screwups by Google - Buzz, the Street View Wi-Fi data collection - and said "The social contract has to be that if you're going to hold on to people's most private data, you have to do a better job of honoring your privacy commitments". He wasn't impressed by Google's explanation that the cookie workaround was unintentional: "As a regulator, it is hard to know which answer is worse: 'I didn't know' or 'I did it deliberately'."

Google's statement, beyond which it's not shifting, is that "We set the highest standards of privacy and security for our users."

But if Rosch was the dissenter, why did the other four think it was OK to let Google off without admitting liability? Here's what they say:

Here, as in all cases, a defendant's denial of liability in a settlement agreement has no bearing on the Commission's determination as to whether it has reason to believe the defendant has violated the law or that a proposed settlement will afford appropriate relief for the Commission's charges. To the contrary, the Commission acts based on its consideration of the staff's investigative work, and in this instance we have strong reason to believe that Google violated its order.

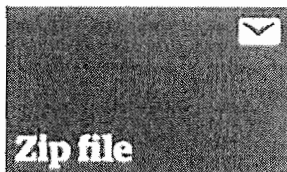
In other words: denying that you killed somebody doesn't cut much ice when you're found holding the knife still in their heart. (Or, less dramatically, denying you ever took those cookies isn't much use when you've been photographed on CCTV with your hand in the cookie jar.)

The key question, the commissioners say, is whether Google will now abide by the consent order. The fine, they imply, is a big whack on the back of the hand for Google "when the accompanying complaint does not allege that the conduct at issue yielded significant revenue or endured for a significant period of time." That's an important point, since there's absolutely no way of knowing how much revenue - if any - Google actually derived from what it did.

Yet simple measures of revenue aren't the key point. What's really important, as Vladeck said, is whether we, as consumers, can trust companies with our data, because our data is becoming all that there is of us (and if you don't believe that, read again about

how [technology writer Matt Honan had his digital life erased](#) by a couple of hackers who wanted access to his Twitter account).

And after this fine, and with the EC still pondering whether it accepts [Google's offerings to solve its antitrust questions](#) over search, and the FTC - them again - [pondering the question of whether Google has abused its dominant position in search](#), and with the Wi-Fi/Street View issue rumbling on in Europe (with the German [data protection](#) authorities considering what action to take, and now the UK's [Information Commissioner's Office doing a forensic examination of the data](#)), and with the [Google Book scanning controversy](#) still rumbling on too, one wouldn't say that Google is out of the woods yet. Even if the FTC's fine represents less than a day's profits, the effects on its reputation could linger for a lot longer.



Get the Guardian's Zip file email

For all you need to know about technology in the world this week, news, analysis and comment.

[Sign up for the Zip file email](#)

[Previous](#)

[Blog home](#)

[Next](#)

More from the guardian

[What makes a language attractive – its sound, national identity or familiarity?](#) 17 Jul 2014

[Dyson Cool AM06 review: is this the world's most luxurious desk fan?](#) 18 Jul 2014

[Student loan system is almost financially unworkable, say MPs](#) 22 Jul 2014

[Facebook closes its \\$2bn Oculus Rift acquisition. What next?](#) 22 Jul 2014

[Will Drip law make UK citizens' data more attractive to hackers?](#) 18 Jul 2014

More from around the web

Promoted content by Outbrain

[If you have Gmail, you need this next-gen email trick](#) (Andrew Skotzko)

[The Latest Killer Extension for Gmail](#) (Forbes)

[DropBox Alternative is Making Join.me Even Better](#) (TechCrunch)

[The IT Tool You Should be Using](#) (VMware)

[10 Video Games That Every Gamer Should Know](#) (Bilibili)

Recommended by

Ads by Google

#1 Extended Auto Warranty

We Pay Parts Labor & 24/7 Roadside. Why Pay Dealer Prices? Free Quote!

[directbuywarranty.com/Free_Quote](#)

Mortgage Forgiveness Plan

Do you Qualify for Mortgage Relief? Check Status Online or Call Us Now.

homereliefprogram.com

[Full BMW Service Center](#)

Let Us Take Care of Your BMW Our Shop is Open 24 Hours a Day

www.bmwofsterling.com

© 2014 Guardian News and Media Limited or its affiliated companies. All rights reserved.

;

From: Johnson, M. Eric <M.Eric.Johnson@tuck.dartmouth.edu>
Sent: Tuesday, April 29, 2008 4:59 PM
To: Chris Gormley <cgormley@tiverson.com>
Subject: RE: WSJ article

Yes, we have concluded that insurance/hmo should be our next subject! I am sitting on an airplane waiting to take off. You around in the am?

E

-----Original Message-----

From: Chris Gormley <cgormley@tiverson.com>
Sent: Tuesday, April 29, 2008 3:43 PM
To: Johnson, M. Eric <M.Eric.Johnson@tuck.dartmouth.edu>
Subject: RE: WSJ article

Eric,

Medical is a treasure trove of information, but it's not necessarily coming from big hospitals. We've got tons of individual practitioners (most notably psychiatrists) who disclose (since they write up their findings).

I'd like to give you a quick call regarding the info - what's your number? I can't find your card right now..

From: Johnson, M. Eric [mailto:M.Eric.Johnson@tuck.dartmouth.edu]
Sent: Tuesday, April 29, 2008 1:27 PM
To: Chris Gormley
Subject: RE: WSJ article

Thanks - I had not seen it yet.

We are coming well on the medical files - finished going through all the files. We are working on the report right now. We turned up some interesting stuff - not as rich as the banks, but I guess that could be expected. Any chance you could share a couple other of your recent medical finds that we could use to spice up the report? You told me about the one database you found that could really boost the impact of the report. Certainly will coordinate with you on the report and release. I forgot to ask - did you guys also grab searches related to our digital signature?

Eric

From: Chris Gormley [mailto:cgormley@tiversa.com]
Sent: Tuesday, April 29, 2008 11:38 AM
To: Johnson, M. Eric
Subject: FW: WSJ article

You've probably seen this, but good read.

From: Robert Boback
Sent: Tuesday, April 29, 2008 11:33 AM
To: Chris Gormley; Griffin Schultz; Katy Everett; John P. Daunt; William Ferguson
Subject: WSJ article

Check out this scanned copy of an article in today's WSJ.

Page 2 is important for agencies that specifically highlight the existing laws around breaches.

Also, it mentions that over 200 CRIMINAL cases have been filed with the DOJ since 2003 regarding HIPAA.....there are consequences for inactivity.

Robert Boback
Chief Executive Officer

Tiversa, Inc.

The Leader in Information Containment Management

144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

Getting it Done II

BUILD A BETTER BOARD

SEE HOW A SOLID BOARD OF DIRECTORS CAN POISE A COMPANY FOR SUCCESS

BY EVAN PATTAK, CONTRIBUTING WRITER

Building an effective board of directors — and a companion advisory board — is a challenging but vital step for young tech companies. This installment of "Getting it Done II" examines how Tiversa, a Cranberry firm that offers data security services, successfully met the challenge by aiming high.

Retired Gen. Wesley Clark, Former eBay COO Maynard Webb, Howard Schmidt, former high-ranking cybersecurity official at the White House, Patrick Gross, Co-Founder of American Management Systems.

If that sounds like an elite force commissioned by the Intergalactic Council, that's exactly what Bob Boback intended. Boback, Tiversa's Co-Founder (with Sam Hopkins) and CEO, landed them all for the firm's advisory board. It was, to say the least, an ambitious undertaking.

"We were focused on getting clients and revenue," Boback says. "So when we considered advisers, we asked ourselves, 'Who can provide introductions? Whose credibility can we leverage to get where we need to be?'"

Because of his high-level marketing experience, Gross was the initial target.

"Getting that first adviser, that beachhead, is the most important

piece," Boback says, "so long as you can get it without giving up too much of the company. That's the ideal situation, and we managed to do that."

Tapping the contacts of its lead Series A investor, Adams Capital Management, Tiversa added the other powerhouses who became stepping-stones to clients . . . and more.

Clark, fresh off his bid for the 2004 Democratic presidential nomination, provided entree to government agencies. Webb helped persuade other eBay stars — former Marketing Chief Michael Dearing, former CTO Lynn Reedy, former Operations Vice President Tom Keegan — to round out Tiversa's seven-member advisory board.

With its advisers leading the way, Tiversa has achieved remarkable success for a company only four years old. Though it won't disclose customer names because of the sensitivity of its business, Tiversa is handling enterprise security for clients that Boback describes as "Global 50," with market capitalizations ranging from \$30 billion to more than \$200 billion.

Its advisory board — and an equally capable board of directors — have been the keys to Tiversa's rapid rise. Here are other lessons

start-ups can learn from Tiversa's board-building success:

DEVELOP A FIRST-RATE PRESENTATION IN MULTIPLE FORMATS

To reel in Schmidt, Tiversa had to persuade him that its technology and team were real, and they had only a single meeting in Washington, D.C. to do the job. Tiversa's presentation was so effective that, at session's end, Schmidt agreed to sign on.

"At this level, you get one shot," Boback notes. "You have to grab them within those first few minutes and prove to them that they need to be with you. Selling to an adviser is just like selling to a client. It can't be just to generate money or leverage their connections. There has to be a story attached. Tell them why you're passionate about what you're doing. They'll feel the passion and gravitate towards it."

Tiversa pitched to Clark through another medium — a WebEx demo. Different format, same results. On the strength of the demo, Clark agreed to a New York meeting and came onboard shortly thereafter.

"Potential advisers don't want blather," says Joel Adams, Founder and General Partner of Adams Capital, who serves on Tiversa's

Getting it Done II

"Potential advisers don't want blather," says Joel Adams, Founder and General Partner of Adams Capital, who serves on Tiversa's board of directors. "They want their time respected. You do that by telling them why they should be interested — and telling them now. You can get to the pleasantries later."

board of directors. "They want their time respected. You do that by telling them why they should be interested — and telling them now. You can get to the pleasantries later."

PLAN — AND BUDGET FOR — BOARD OPTION PACKAGES

Although the company was prepared to customize equity offers to meet the needs of its talented advisers, the standard package Tiversa developed proved to be satisfactory. That enabled Tiversa to stick to its budgeted numbers for options — an important consideration, since it anticipates offering additional options in future funding rounds.

Remember also that if you grant options down the road, whether to investors, directors or staff, the equity of the earliest investors and board

members likely will be diluted.

Observes Boback:

"Nobody wins with dilution unless we can point to the fact that raising more capital will generate more revenue more quickly, so that in the long run, your percentage of the company, although a smaller number, is worth more. Advisers don't want to dilute, so they'll do whatever they can to make this company successful."

KEEP YOUR BOARD OF DIRECTORS NIMBLE

Significant outside investment usually brings with it the need to formalize a board structure that may have been loose in the formative months. Tiversa turned to its counsel, Morgan, Lewis & Bockius, to create that structure and accompanying documents.

"Yes, you need the formality and the papers," confirms Eric Kline of Morgan Lewis. "But more than anything you need chemistry. Tiversa's board members are world-class, each adding valuable insight, the whole functioning cohesively."

The size and tenor of the board facilitate its effective operation. Tiversa opted for a three-member board — Boback, Adams and company CFO Dave Becker — with the option to expand up to five. It's a board that's geared for decisive action.

"Collegiality should be the order of the day, as should mutual respect," Adams says. "I prefer odd numbers to even for obvious reasons, smaller to bigger. With small boards, you can make decisions quickly. Many times, there's no rocket science involved. It's just a matter of getting the facts on the table, using good, sound judgment and pulling the trigger."

KEEP YOUR DIRECTORS UP TO SPEED

"One of the things that drives me crazy about boards," Adams says, "is when you walk into a meeting and management spends the whole time getting everybody up to the same information level. Entrepreneurs need to keep everybody up to speed so directors start from a base of common knowledge and actually perform work from there."

Tiversa's board meets bimonthly, but the directors keep in touch on a daily basis, or very nearly so.

"I couldn't wait two months to say, 'Here's what's happening,'" Boback explains. "There are events occurring here and now, and I need a decision today."

PUT YOUR BOARDS TO WORK

You engaged your directors and advisers for their expertise. Deploy those assets by tasking your boards with specific missions tailored to their talents.

"Some companies use advisory boards as window dressing," Adams says. "The interaction is minimal, and that type of board isn't worth much. Tiversa has been able to get its advisers to interact, to participate. When they walk out of a board meeting, they have to-do lists."

On the other hand, neither you nor your board wants directors to micro-manage the business. Board-level assignments make sense, but as Adams puts it:

"If I have to be active in the operations, there's a problem." ○

Tiversa Identifies Over 13 Million Breached Internet Files in the Past Twelve Months

Tiversa today announced the findings of new research that revealed 13,185,252 breached files emanating from over 4,310,839 sources on P2P file-sharing networks within a twelve month period from March 01, 2008 - March 01, 2009. This new data clearly demonstrates that P2P file-sharing risk is not effectively being addressed by the security protocols of Fortune 500 companies and government agencies, as these organizations commonly have exposure across the Extended Enterprise. Tiversa's findings also hint at the enormity of the issue at hand.

Cranberry Township, PA (PRWEB) May 28, 2009 -- Tiversa today announced the findings of new research that revealed 13,185,252 breached files emanating from over 4,310,839 sources on P2P file-sharing networks within a twelve month period from March 01, 2008 - March 01, 2009.

The research is based on data in an ongoing study by Tiversa, whose patent-pending technology monitors roughly 450 million users issuing more than 1.5 billion searches a day. The files analyzed included only those identified on behalf of Tiversa's existing customer base during the 12 month period. It's also important to note that the referenced files are business documents only (.doc, .xls, .pdf, .pst, etc). Music, software and movie files (.avi, .mov, .wma, .mpeg4, .mp3, etc) were not included in the study.

This new data clearly demonstrates that P2P file-sharing risk is not effectively being addressed by the security protocols of Fortune 500 companies and government agencies, as these organizations commonly have exposure across the Extended Enterprise. Tiversa's findings also hint at the enormity of the issue at hand.

"P2P file-sharing presents a broad spectrum risk to organizations of all shapes and sizes. This is a horizontal issue occurring across all verticals", says Robert Boback, Tiversa CEO. "The information being shared across these networks is staggering. In a typical day, Tiversa might see the Protected Health Information (PHI) of tens of thousands being disclosed by a hospital or medical billing company, the Personally Identifiable Information (PII) of an organization's global workforce being exposed through a third-party payroll provider and a Fortune 500 company exposing corporate IP, such as pre-patent documentation or executive board minutes."

Tiversa's latest research reinforces warnings aired in recent media reports, as well as, growing concerns voiced by Congress in new legislative discussions aimed at protecting consumers by requiring stricter privacy and security procedures around computerized data containing personal information (H.R. 2221 Data Accountability and Trust Act).

Findings released in February 2009, in a collaborative research study (Data Hemorrhages in the Health-Care Sector) between Tiversa and The Tuck School of Business at Dartmouth College highlight these same risks by focusing on the exposure rate of sensitive data in the healthcare industry.

Over a two-week period, Dartmouth College researchers and Tiversa searched file-sharing networks for key terms associated with the top ten publicly traded health care firms in the country, and discovered a treasure trove of sensitive documents. Found was a spreadsheet from an AIDS clinic with 232 client names, including Social Security numbers, addresses and birth-dates. Discovered were databases for a hospital system that contained detailed information on more than 20,000 patients, including Social Security numbers, contact



details, insurance records, and diagnosis information.

Also identified was a 1,718-page document from a medical testing laboratory containing patient Social Security numbers, insurance information, and treatment codes for thousands of patients, as was 350+ megabytes of data comprising sensitive reports relating to patients of a group of anesthesiologists.

In today's world of open communication, one of the greatest challenges privacy, information security and risk management professionals face is how to provide open and direct access to information while protecting sensitive and confidential documents. Tiversa has seen millions of individual records and sensitive files inadvertently being shared by organizations, their agents, key suppliers, and trusted partners. This type of confidential information is continuing to be exposed and risks being used for competitive intelligence, fraud, identity theft, medical identity theft and criminal gain.

Tiversa provides P2P Intelligence and Security Services to corporations, government agencies and individuals based on patent pending technologies that can monitor over 450 million users issuing 1.5 billion searches a day. Requiring no software or hardware, Tiversa detects, locates and identifies exposed files in real-time, while assisting in remediation and prevention efforts.

For more information on Tiversa, their solutions or research, please contact them at (724) 940-9030 or [visit online](#).

###



Contact Information

Scott Harrer

Iiversa

<http://www.iiversa.com>

724-940-9030

Online Web 2.0 Version

You can read the online version of this press release [here](#).

COLUMBIA JOURNALISM REVIEW

Strong Press, Strong Democracy

The Audit — February 9, 2011 07:02 PM

Bloomberg and *BusinessWeek*'s Problematic WikiLeaks Story

Red flags aflutter as the news outfit runs with seriously questionable evidence

By Ryan Chittum

How many red flags can we count in this *Bloomberg BusinessWeek* piece on WikiLeaks?

First there's the headline:

Is Wikileaks Hacking For Secrets?

I, like my colleague Lauren Kirchner, have a real problem with question headlines, which seem to have proliferated in recent years. On the bright side, they're good leads for critics like us: It's a sure sign that the reporter can't answer the question and a possible sign that they shouldn't have written the piece in the first place. In this case it turns out to be both.

The second red flag is the subhed:

Internet security company Tiversa says WikiLeaks may be exploiting a feature in peer-to-peer file-sharing applications to search for classified data

"Internet security company Tiversa says," huh? Who the heck is Tiversa? It ain't exactly McAfee or whatever.

More importantly, an Internet security company has an incentive to pitch stories that make it seem like Internet security is really, really bad. That way you'll buy their services. Here's how Tiversa describes what it does:

Tiversa provides P2P Intelligence and Security services to corporations, government agencies and individuals based on patented technologies that can monitor over 500 million users issuing 1.6 billion searches a day.

The third flag is all the weasel words in the key paragraph explaining the "evidence" (emphasis is mine):

Except that WikiLeaks, according to Internet security company Tiversa, **appears to have** hunted down that military document itself. Tiversa says the group **may have** exploited a feature of file-sharing applications **such as** LimeWire and Kazaa that are often used to swap pirated copies of movies and music for free. **If**, for example, a Pentagon employee were to log on to such a peer-to-peer network (an array of disparate computers with no central hub) to download a movie, he **could possibly** expose every last e-mail and spreadsheet on his PC to prying eyes. That's because **some** peer-to-peer, or P2P, applications **may** scan users' hard drives for shareable files. Not turning that feature off, or specifying which parts of the hard drive may be searched, leaves the door wide open.

Hmm. So a P2P security company says Wikileaks "appears to have" hacked into military computers and "may have" used P2P to do it. What's wrong with this picture?

And *BBW* (the story originally ran at Bloomberg) continues on with its reckless speculation via weasel word:

The possibility that the site is systematically ransacking computers may offer prosecutors an alternate path to get the group and its founder into a U.S. courtroom.

Neatly enough for Tiversa, *BizWeek* plays along with the cloak and dagger stuff:

To conduct a massive search of networks around the world, huge amounts of computing horsepower and bandwidth are required.

Tiversa has plenty of both. In a secure room at the company's headquarters in Cranberry Township, Pa., banks of servers create a minute-by-minute map of what is effectively a global treasure trove of secrets. In a brief demonstration of what's out there for the taking, a Tiversa analyst taps a few keys, and up pops the cell phone number of actress Lucy Liu along with the pseudonym she uses to check into hotels—attached to a production company document clearly labeled "not to be made public." There are several draft chapters of a book by white supremacist David Duke, as well as a spreadsheet of all the donors to his cause. Assange has told interviewers that his group has damaging information on pharmaceutical, energy,

and financial companies; (Tiversa CEO Robert) Boback confirms that confidential corporate documents are readily accessible.

Cut to PR executives high-fiving.

Fourth red flag: It's essentially a one-source story. Here's the evidence Bloomberg presents as if it's fact (you'll see below that it's not):

In the missile-range case, Tiversa's systems noticed unusual activity coming from a cluster of computers in Sweden, where until December WikiLeaks had some of its key servers. The cluster was furiously searching P2P networks around the world. It hit pay dirt in the form of a file blandly labeled BPL_HL.pdf, available for download from a computer in Hawaii. The Swedish computers downloaded the document, and two months later it was posted on WikiLeaks.

Executives at Tiversa, which is hired by governments and corporations to use the same loophole to find exposed documents and figure out who might be accessing them, say the Hawaii incident wasn't an isolated case. Its technology has detected the mysterious Swedish computers downloading gigabytes of data, much of which soon appeared on WikiLeaks. "WikiLeaks is doing searches themselves on file-sharing networks," says Robert Boback, Tiversa's chief executive officer. "It would be highly unlikely that someone else from Sweden is issuing those same types of searches resulting in that same type of information."

The fifth sorta-kinda red flag (once you've seen two or three in one piece, it's good to start suspecting everything in it) is that two of Tiversa's advisors have awfully tight ties to the U.S. military and federal government. Wesley Clark, the former NATO commander and four-star general, is an advisor as is Howard Schmidt, who worked for the feds for three decades. Here's the latter's bio:

He retired from the White House after 31 years of public service in local and federal government including the Air Force Office of Special Investigations and the FBI National Drug Intelligence Center. He was appointed by President Bush as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House in December 2001.

This piece raised questions from *Forbes*'s Andy Greenberg, too, and he beat me to it by more than two weeks. It's some excellent blogging.

Sure enough, Greenberg confirms that Tiversa is working for the U.S. government, which is Wikileaks's sworn enemy, and he blows apart Bloomberg's piece with this reporting:

In fact, in a phone interview with me today, Boback sounded distinctly less sure of his firm's deductions than he did in the Bloomberg piece. "What we saw were people who were searching [computers connected to filesharing networks] for .xls, .doc, .pdf, and searching for those generic terms over and over again," says Boback. "They had multiple Swedish IPs. Can I say that those are WikiLeaks? I can't. But we can track the downloads of people doing that, and a short time after those files were downloaded, they're listed on WikiLeaks."

Boback, who says he's working with a U.S. government investigation into possible peer-to-peer sources for WikiLeaks, says that he saw downloads of documents that later were posted to WikiLeaks from other countries too, both "in the U.S. and across Europe." "Many of the searches are in Sweden, many are outside," adds Boback. "It's hard for us to say that any IP address was WikiLeaks."

Ayy.

And then there's the Occam's Razor thing, which should have raised some questions from editors somewhere along the way:

Still, WikiLeaks' latest bombshells, like the military documents and State Department cables allegedly leaked by Bradley Manning and the upcoming list of tax-sheltered Julius Baer clients in Switzerland, seem to have been the product of traditional whistleblowing, not hacking. Part of what has made WikiLeaks so much more effective than traditional hacking efforts, after all, is that whistleblowers with privileged accounts within computer networks are a far more efficient source of embarrassing data than hacking techniques such as random searches of filesharing networks. As Assange reminded me when we spoke in November: "Insiders know where the bodies are."

The unfortunate bottom line is that it seems the press feels freer to go aggressively after enemies of the state, even if they're helping it do its job informing the people about what their state is doing in their name.

Would this kind of journalism have passed the smell test if it weren't about Wikileaks? I highly doubt it.

Bloomberg and *BusinessWeek* shouldn't have run with this one. It looks for all the world that they may (to borrow a word) have published a smear.



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

Alain Sheer
Attorney
Division of Privacy and Identity Protection

Direct Dial: 202.326.3321
Fax: 202.326.3629
E-mail: ashoor@ftc.gov

January 19, 2010

Via Federal Express

Michael J. Daugherty
LabMD, Inc.
2030 Power Ferrys Road
Bldg. 500, Suite 520
Atlanta, GA 30339

Dear Mr. Daugherty:

As I discussed today with Mr. Boyle, the staff of the Federal Trade Commission ("Commission") is conducting a non-public inquiry into LabMD, Inc.'s compliance with federal law governing information security. According to information we have received, a computer file (or files) from your computer network is available to users on a peer-to-peer file sharing ("P2P") network (hereinafter, "P2P breach").¹ The file (or files) contains sensitive information about consumers and/or employees that could be used to commit identity theft or fraud or cause other types of harms to consumers and/or employees.²

Section 5 of the FTC Act prohibits deceptive or unfair acts or practices, such as misrepresentations about privacy and security and practices that cause substantial injury to

¹ P2P networks are created when users install compatible peer-to-peer file sharing applications on personal computers in homes and businesses. The applications link these computers together and can be used to share files between the computers. Once a file has been shared, the original source of the file cannot remove the file from the P2P networks or control access to it by other users on the networks.

For information about security concerns raised by the use of peer-to-peer file sharing applications and possible responses to them, see the enclosed *Peer-to-Peer File Sharing: A Guide For Business*, www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

² One such file is *insuranceaging_6.05.071*.

consumers.³ Accordingly, we seek to determine whether your handling of sensitive information from or about consumers and/or employees raises any issues under Section 5.

We invite you to meet with us in our Washington, D.C. office to discuss this matter, or to discuss this matter with us by telephone. If possible, we would like to meet during the week of March 8, 2010. In advance of the meeting, we request that you provide us with the information and documents listed below by February 22, 2010. Please feel free to submit any additional information you believe would be helpful to the Commission's understanding of this matter. Any materials you submit in response to this request, and any additional information that you mark "Confidential," will be given confidential treatment.⁴

In preparing your response:

- Please provide all responsive documents in the possession, custody, or control of LabMD, and its parents, owners, subsidiaries, divisions, affiliates, branches, joint ventures, and agents (collectively, "LabMD", "you," or "your").
- Please submit complete copies of all documents requested, even if you deem only part of a document to be responsive.
- Responses to each request should describe in detail each material change or update that has been made that concerns, refers, or relates to the request, as well as the date the change or update was implemented and the reason(s) for the change or update.
- Please number each page of your response by Bates stamp or otherwise, and itemize your response according to the numbered paragraphs in this letter.
- If any document is undated, please indicate in your response the stamped page numbers of the document and the date on which you prepared or received it.
- If you do not have documents that are responsive to a particular request, please submit a written statement in response. If a document provides only a partial response, please submit a written statement which, together with the document, provides a complete response.
- If you decide to withhold responsive material for any reason, including an applicable privilege or judicial order, please notify us before the date set for

³ 15 U.S.C. § 45 *et seq.*

⁴ The Commission's procedures concerning public disclosure and confidential treatment can be found at 15 U.S.C. §§ 46(f) and 57b-2, and at Commission Rules 4.10 - 4.11 (16 C.F.R. §§ 4.10 - 4.11).

responding to this request and submit a list of the items withheld and the reasons for withholding each.

- Please do not submit documents that contain any individual consumer's or employee's date of birth, Social Security number, driver's license or other personal identification number, financial account information, or medical information. If you have responsive documents that include such information, please redact the information before providing the documents.
- We may seek additional information from you at a later time. Accordingly, you must retain all relevant records, documents, and materials (not only the information requested below, but also any other information that concerns, reflects, or relates to this matter, including files and information stored electronically, whether on computers, computer disks and tapes, or otherwise) until the final disposition of this inquiry or until the Commission determines that retention is no longer necessary.⁵ This request is not subject to the Paperwork Reduction Act of 1980, 44 U.S.C. § 3512.
- A responsible corporate officer or manager of LabMD shall sign the responses and certify that the documents produced and responses given are complete and accurate.
- For purposes of this letter, the term "personal information" means individually identifiable information from or about an individual consumer, including, but not limited to: (a) first and last name; (b) home or other physical address, including street name and name of city or town; (c) email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) telephone number; (e) date of birth; (f) government-issued identification number, such as a driver's license, military identification, passport, or Social Security number, or other personal identification number; (g) financial information, including but not limited to: investment account information; income tax information; insurance policy information; checking account information; and credit, debit, and/or check-cashing card information, including card number, expiration date, security number (such as card verification value), information stored on the magnetic stripe of the card, and personal identification number; (h) health information, including, but not limited to: prescription medication and dosage; prescribing physician name, address, and telephone number; health insurer name, and insurance account and policy numbers; and medical condition or diagnosis; (i) employment information, including, but not limited to, income, employment, retirement, disability, and medical records; (j) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is

⁵ Failure to retain documents that may be relevant to this matter may result in civil or criminal liability. 15 U.S.C. § 50.

combined with other available data that identifies an individual consumer; or (k) any information from or about an individual consumer that is combined with any of (a) through (j) above. For the purpose of this definition, an individual consumer shall include an "employee", and "employee" shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under your control.

REQUESTS FOR DOCUMENTS AND INFORMATION

Please provide the documents and information identified below.⁶ Unless otherwise indicated, the time period covered by these requests is from January 1, 2007 through the date of full and complete production of the documents and information requested.

General Information

1. Identify the complete legal name of LabMD and all other names under which it does, or has done, business, its corporate mailing address, and the date and state of incorporation.
2. Identify and describe LabMD's parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchises, operations under assumed names, and entities over which it exercises supervision or control. For each such entity, describe in detail the nature of its relationship to LabMD.
3. Identify each individual or entity having an ownership interest in LabMD, as well as their individual ownership stakes and their positions and responsibilities within LabMD.
4. Provide documents sufficient to describe your business in detail. The response should identify and describe: each product and service you offer; each location (both online and offline) through which you offer such products and services; and, annually, your revenue, number of employees, and number of customers.

Personal Information

5. Provide documents that describe in detail the types of personal information you collect,

⁶ For purposes of this letter: the word "any" shall be construed to include the word "all," and the word "all" shall be construed to include the word "any;" the word "or" shall be construed to include the word "and," and the word "and" shall be construed to include the word "or;" the word "each" shall be construed to include the word "every," and the word "every" shall be construed to include the word "each;" and the term "document" means any preexisting written or pictorial material of any kind, regardless of the medium in which such material was created, and regardless of the method by which it is stored (e.g., computer file, computer disk or tape, microfiche, etc.).

obtain, store, maintain, process, transmit, handle, or otherwise use (collectively, "collect and store") in conducting your business, how and where you collect and store the information, and how you use the information. The response should include, but not be limited to: documents sufficient to identify the type(s) of personal information you collect and store, the source(s) of each such type of information (such as consumers, employees, medical providers, healthcare plans, and insurance companies), and the manner by which you collect or obtain the information (such as by paper documents or electronically through a website); and documents or a narrative that describe in detail how you use each type of information in conducting your business.

Security Practices

6. Identify by name, location, and operating system each computer network that you use directly or indirectly to collect and store personal information, and provide for each such network:
 - (a) a high-level diagram (or diagrams) that sets out the components of the network and a narrative that describes the components in detail and explains their functions and how they operate together on the network. The description of the network components should identify and locate (within the network): computers; servers; firewalls; routers; internet, private line, and other connections; connections to other internal and external networks; virtual private networks; remote access equipment (such as wireless access points); web sites; and security mechanisms and devices (such as intrusion detection systems). In responding, please feel free to use blueprints and diagrams that set out in detail the components, topology, and architecture of the network;
 - (b) documents sufficient to identify each computer, server, or other device where you collect and store personal information and, for each such computer, server, or device, each program, application, or other means (collectively, "databases") used to collect and store personal information; and
 - (c) documents that concern, relate, or refer to each database identified in the response to Request 6(b), including, but not limited to: operating manuals; user guides; communications with database vendors; database schemes, diagrams, and/or blueprints (including table and field names); and documents sufficient to identify the length of time for which you maintain personal information in the database.
7. Provide documents or a narrative that describe in detail the flow path of personal information over each network identified in response to Request 6, including the initial collection point for personal information (such as a website), the entry and exit points to and from the network, and all intermediate points within the network.
8. Provide documents sufficient to identify the policies, procedures, and practices you have used on each network identified in the response to Request 6 to prevent unauthorized

access to personal information collected and stored on the network, as well as the time period during which such policies, procedures, and practices were written and implemented. The response should include, but not be limited to, documents that concern, reflect, or relate to: controls on direct or remote access to personal information (such as a firewall policy or a password policy); controls on accessing and/or downloading personal information without authorization; the lifecycle of personal information, including maintaining, storing, using, and/or destroying the information; controls on the installation of programs or applications on computers or work stations on the network by employees or others; limits on the transmission of personal information within the network and between the network and other (internal or external) networks; logging network activity and reviewing the logs; secure application and website development; employee training; and plans for responding to security incidents.

9. For each network identified in the response to Request 6, provide documents that describe in detail each security policy, procedure, practice, control, defense, or other measure (collectively, "security practice") used on the network. The response should include, but not be limited to:
- (a) all documents that concern, reflect, or relate to each security practice, including, but not limited to, practices to control the installation and/or use of P2P programs (whether such programs are authorized or not);
 - (b) documents that set out the technical configurations of devices and programs you use to enforce each security practice, including, but not limited to, the configurations of firewalls or other means used to control or block P2P communications to and from the network and networks that connect to it;
 - (c) training or security awareness materials provided to network users (such as employees and third-party persons and entities with access to the network) regarding your security practices, such as materials that concern security generally or the use of and risks presented by P2P programs;
 - (d) documents that set out the frequency and extent to which such network users receive training or security awareness materials generally and as to the use of and risks presented by P2P programs;
 - (e) documents sufficient to identify by name and title each employee who is, or has been, responsible for coordinating security practices on the network, and to describe the responsibilities of each such employee;
 - (f) documents sufficient to identify whether and, if so, when you conducted or obtained (from another person or entity) a risk assessment to identify risks to the security, integrity, and confidentiality of personal information on the network;
 - (g) all documents that concern, reflect, or relate to testing, monitoring, and/or

evaluations of the effectiveness of security practices used on the network, including the dates when such activities were conducted and completed and plans and procedures for future testing, monitoring, and/or evaluation of security practices; and

- (h) documents that set out in detail all changes made to security practices on the network based upon testing, monitoring, and/or evaluations identified in the response to Request 9(g).

10. Provide all documents that concern, reflect, or relate to each risk assessment identified in the response to Request 9(f) and the security risks identified therein, if any. For each such assessment, the response should include, but not be limited to:

- (a) documents sufficient to identify the date of the assessment and the name and title of the person(s) responsible for conducting the assessment;
- (b) a copy of the assessment;
- (c) documents that describe in detail the steps taken in conducting the assessment;
- (d) documents that concern, reflect, or relate to specific risks identified in the assessment and how you addressed each such risk; and
- (e) a copy of each (internal or external) report or other document that verifies, confirms, challenges, questions, or otherwise concerns the assessment.

11. Provide documents sufficient to identify each third-party person or entity that, in the course of providing services to you ("service provider"), receives, maintains, processes, or otherwise is permitted access to personal information collected and stored by you.

12. For each service provider identified in the response to Request 11, provide:

- (a) documents sufficient to identify the types of personal information to which the service provider has access;
- (b) documents sufficient to describe the manner and form of the service provider's access to personal information (such as physical access to your offices, remote access to your computer network(s), or the mailing of paper documents or computer storage media);
- (c) a narrative that explains in detail the business reasons why the service provider has access to such information;
- (d) copies of all contracts between you and the service provider;

- (e) documents that describe in detail the measures you took to select and retain the service provider to ensure that it is capable of appropriately protecting personal information you have provided or made available to the service provider; and
- (f) documents that describe in detail how you monitor the service provider to confirm that it has implemented and maintained security measures adequate to protect the security, integrity, and confidentiality of such personal information.

Other Information

13. Provide documents sufficient to identify any instance of which you are aware (including, if appropriate, the P2P breach) where personal information from a network identified in the response to Request 6 was or may have been shared or accessed without authorization (the "intrusion"), and, for each such intrusion, identify when and how you first learned about the intrusion, the network(s) involved, and all persons with knowledge about it.
14. Separately for each intrusion identified in the response to Request 13, provide all documents prepared by or for you that identify, describe, investigate, evaluate, or assess:
 - (a) how the intrusion occurred;
 - (b) the time period over which it occurred;
 - (c) the security vulnerabilities that were or may have been exploited in the intrusion;
 - (d) the actual or suspected point of entry;
 - (e) the path the intruder followed from the (actual or suspected) point of entry to the location of the personal information that was or may have been compromised and then in exporting or downloading the information (including all intermediate points);
 - (f) the type(s) and amount(s) of personal information that was or may have been accessed without authorization; and
 - (g) the security measures you implemented in response to the intrusion.

Responsive documents should include, but not be limited to: preliminary, interim, draft, and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in the intrusion; (formal and informal) security audits or forensic analyses of the intrusion prepared internally and by third parties; security scans (such as for packet capture tools, password harvesting tools, rootkits, P2P programs, and unauthorized programs); incident reports; documents that identify the intruder; logs that record the intruder's steps in whole or part in conducting the intrusion; warnings issued by anti-virus, intrusion detection, or other security measures; records of reviews by

network administrators or others of logs and warnings; records setting out the routine security activities and checklists performed by network administrators (such as verifying that scheduled jobs were authorized); and other documents that concern, reflect, or relate to the intrusion, such as minutes or notes of meetings attended by you or your employees.

15. Separately for each intrusion identified in the response to Request 13 that was accomplished or facilitated by a P2P program and for the P2P breach if not identified in the response to Request 13 ("collectively, "P2P intrusion"), identify each P2P program (including version number and upgrade) that was, or may have been, used in any way in the intrusion. For each such program:
 - (a) identify: the manufacturer, model, type, operating system, and network location of each computer or other electronic device on which the P2P program was installed (collectively, the "breach computer"); the source from which the program was downloaded to the breach computer; when and by whom the program was downloaded and installed on the breach computer; when the program was removed from the breach computer; how long the program was active on the computer; whether the default settings on the program were changed after it was installed on the breach computer, and, if so, when, by whom, and in what ways; and whether you authorized the installation and use of the program on the breach computer;
 - (b) explain in detail your business need for using the program, if any, and identify who was using the program and why they were using it;
 - (c) explain in detail all limitations you placed on use of the program, including security practices; and
 - (d) provide a copy of each file generated as a result of installing the program on the breach computer, including, but not limited to, executable, history, and configuration files.
16. Separately for each P2P intrusion:
 - (a) provide all logs, audits, assessments, or reports that concern, reflect, or relate to the intrusion;
 - (b) identify the name of each folder and subfolder that was shared (uploaded or downloaded) through the intrusion, the name (including file extension) and content of each internal and external file (other than a purely music or video file) that was shared, and the amount and type of personal information in each file that was shared; and
 - (c) describe in detail each folder, subfolder, file, and/or program (including functionality) that was shared through the intrusion.

17. Separately for each intrusion identified in the response to Request 13, provide all documents that concern, relate, or refer to fraud and/or identity theft attributable to the intrusion and to the consequences of the fraud or identity theft. Responsive documents should include, but not be limited to:
- (a) fraud reports, alerts, or warnings issued by bank associations, banks, or other entities; documents that assess, identify, evaluate, estimate, or predict the number of consumers or employees that have, or are likely to, suffer fraud or identity theft; claims made against you for fraud or identity theft, such as by affidavits filed by consumers or employees; and documents that assess, identify, evaluate, estimate, or predict the dollar amount of fraud, identity theft, or other costs (such as for increased fraud monitoring or providing fraud insurance) attributable to the intrusion;
 - (b) documents that concern, reflect, or relate to investigations of or complaints filed with or against you relating to the intrusion, including, but not limited to, private lawsuits, correspondence with you, and documents filed with Federal, State, or local government agencies, Federal or State courts, and Better Business Bureaus; and
 - (c) documents or a narrative that identifies how (such as by public announcement or individual breach notification letter), when, how many, and by whom consumers and/or employees were notified that their personal information was or may have been obtained without authorization through the intrusion. If notification has been made, explain why notification was made (e.g., compelled by law) and provide a copy of each substantively different notification. If notification was not provided as soon as you became aware of the intrusion or was not provided to all affected consumers and/or employees or at all, provide a narrative explaining why not.
18. Provide documents sufficient to identify all policies, claims, and statements you have made regarding the collection, disclosure, use, storage, destruction, and protection of personal information, including any policies, claims, or statements relating to how you secure personal information, and for each such policy, claim, or statement identify the date(s) when it was adopted or made, to whom it was distributed, and all means by which it was distributed.

Please send all documents and information to: Alain Sheer, Division of Privacy and Identity Protection, Federal Trade Commission, 600 Pennsylvania Ave., NW, Mail Stop NJ-8122, Washington, D.C. 20580. Due to extensive delays resulting from security measures taken to ensure the safety of items sent via the U.S. Postal Service, we would appreciate receiving these materials via Federal Express or a similar delivery service provider, if possible.

Thank you for your prompt attention to this matter. Please contact me (at 202.326.3321)

if you have any questions about this request or need any additional information.⁷

Sincerely,



Alain Sheer
Division of Privacy and Identity Protection

⁷ The Commission has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REQFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action. The Commission strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

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.



PROTECT YOURSELF FROM SCAMS AND FRAUD

MAIN MENU

SEARCH

FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy

Commission Alleges Exposure of Medical and Other Sensitive Information Over Peer-to-Peer Network

FOR RELEASE

August 29, 2013

TAGS: Health Care | Health Professional Services | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security | Health

The Federal Trade Commission filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company failed to reasonably protect the security of consumers' personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers.

The complaint alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves.

The case is part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers' personal data.

LabMD conducts laboratory tests on samples that physicians obtain from consumers and then provide to the company for testing. The company, which is based in Atlanta, performs medical testing for consumers around the country. The Commission's complaint alleges that LabMD failed to take reasonable and appropriate measures to prevent unauthorized disclosure of sensitive consumer data – including health information – it held. Among other things, the complaint alleges that the company:

- did not implement or maintain a comprehensive data security program to protect this information;
- did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to this information;
- did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;

did not adequately train employees on basic security practices; and

did not use readily available measures to prevent and detect unauthorized access to personal information.

The complaint alleges that a LabMD spreadsheet containing insurance billing information was found on a P2P network. The spreadsheet contained sensitive personal information for more than 9,000 consumers, including names, Social Security numbers, dates of birth, health insurance provider information, and standardized medical treatment codes. Misuse of such information can lead to identity theft and medical identity theft, and can also harm consumers by revealing private medical information.

P2P software is commonly used to share music, videos, and other materials with other users of compatible software. The software allows users to choose files to make available to others, but also creates a significant security risk that files with sensitive data will be inadvertently shared. Once a file has been made available on a P2P network and downloaded by another user, it can be shared by that user across the network even if the original source of the file is no longer connected.

"The unauthorized exposure of consumers' personal data puts them at risk," said Jessica Rich, Director of the FTC's Bureau of Consumer Protection. "The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate security measures to prevent it from falling into the hands of identity thieves and other unauthorized users."

The complaint also alleges that in 2012 the Sacramento, California Police Department found LabMD documents in the possession of identity thieves. These documents contained personal information, including names, Social Security numbers, and in some instances, bank account information, of at least 500 consumers. The complaint alleges that a number of these Social Security numbers are being or have been used by more than one person with different names, which may be an indicator of identity theft.

The complaint includes a proposed order against LabMD that would prevent future violations of law by requiring the company to implement a comprehensive information security program, and have that program evaluated every two years by an independent, certified security professional for the next 20 years. The order would also require the company to provide notice to consumers whose information LabMD has reason to believe was or could have been accessible to unauthorized persons and to consumers' health insurance companies.

The Commission vote to issue the administrative complaint and notice order was 4-0.

Because LabMD has, in the course of the Commission's investigation, broadly asserted that documents provided to the Commission contain confidential business information, the Commission is not publicly releasing its complaint until the process for resolving any claims of confidentiality is completed and items in the complaint deemed confidential, if any, are redacted.

NOTE: The Commission issues an administrative complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. The issuance of the administrative complaint marks the beginning of a proceeding in which the allegations will be tried in a formal hearing before an administrative law judge.

The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. To file a complaint in English or Spanish, visit the FTC's online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357). The FTC enters complaints into Consumer Sentinel, a secure, online database available to more than 2,000 civil and criminal law enforcement agencies in the U.S. and abroad. The FTC's website provides free information on a variety of

consumer topics. Like the FTC on Facebook, follow us on Twitter, and subscribe to press releases for the latest FTC news and resources.

CONTACT INFORMATION

MEDIA CONTACT:

Jay Mayfield
Office of Public Affairs
202-326-2181

STAFF CONTACT:

Robert Schoshinski
Bureau of Consumer Protection
202-326-3219



EVENTS CALENDAR

Related Cases

LabMD, Inc., In the Matter of

For Consumers

How To Keep Your Personal Information Secure

Identity Theft

Media Resources

Our Media Resources library provides one-stop collections of materials on numerous issues in which the FTC has been actively engaged. These pages are especially useful for members of the media.

[Contact Us](#)

[About Us \(PDF\)](#)

[Privacy Policy](#)

[Open Access Policy](#)

ABOUT THE FTC

THE NEED FOR LIMITS ON AGENCY DISCRETION & THE CASE FOR SECTION 5 GUIDELINES

Commissioner Joshua D. Wright*
Federal Trade Commission
December 16, 2013
Washington, D.C.

* The views expressed in this presentation are my own and do not necessarily reflect the views of the Commission or any other Commissioner.



Overview

- Limits on Agency Discretion Generally
- Identifying the Section 5 Problem
- Need for Limits on Section 5 Still Exist
- Selecting a Principled Section 5 Standard



Limits on Agency Discretion

- Why Should An Agency Limit its Discretion?
- Primary and obvious cost: loss of flexibility
- Some Benefits:
 - Enforcement credibility
 - Ability to influence and comment on existing law
 - Educate judges
 - Minimizing political risks
- Examples: FTC experience with deception, unfairness, mergers



Identifying the Section 5 Problem

- Gap between Section 5 in theory and practice stems in part from the vague and ambiguous nature of the FTC's authority under the statute
- Section 5 today is as broad or as narrow as a majority of Commissioners believes it is
- Businesses cannot distinguish lawful conduct from unlawful conduct without guidance



Identifying the Section 5 Problem

No responsive competition policy can neglect the social and environmental harms produced as by-products of the marketplace: resource depletion, energy waste, environmental contamination, worker alienation, the psychological and social consequences of producer-stimulated demands.

-- Former Chairman Michael Pertschuk (1977)



Identifying the Section 5 Problem

An unfair method of competition includes:

actions that are collusive, coercive, predatory, restrictive, or deceitful, or otherwise oppressive, and do so without a justification that is grounded in legitimate, independent self-interest. (emphasis added)

-- Former Chairman Jon Leibowitz (2006)



Identifying the Section 5 Problem

- Uncertainty surrounding scope of Section 5 is exacerbated by the administrative process advantages available to the FTC
- In the past nearly 20 years, FTC has ruled in favor of Staff on appeal in 100% of cases
- Win rate for antitrust plaintiffs appealing from district court is closer to 50%

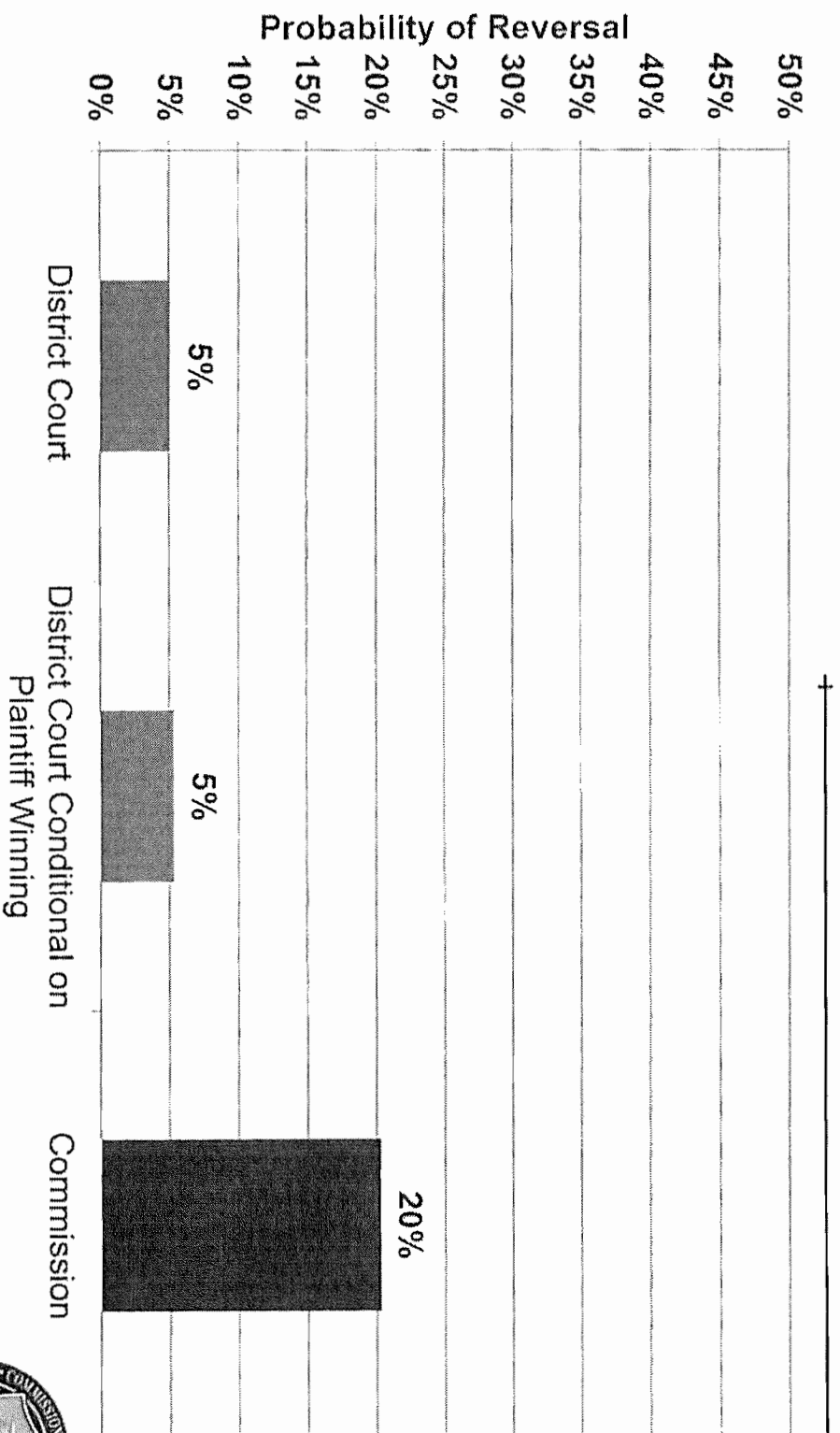


Identifying the Section 5 Problem

- Two hypotheses to explain the 100% win rate on appeal to the Commission are:
 - Commission expertise over private plaintiffs in picking winning cases; and
 - Institutional and procedural advantages for the Commission in administrative adjudication
- Treatment of FTC decisions by courts of appeal puts expertise hypothesis into doubt



Identifying the Section 5 Problem



Identifying the Section 5 Problem

- Combination of the FTC's administrative process advantages with Section 5's vague and ambiguous scope enables easy consents
- Litigation unlikely where the Section 5 standard is a moving target and respondents appear to have the chips stacked against them
- Section 5 scope can account for the institutional differences between federal courts and agencies



Need for Limits on Section Still Exist

- Some today still argue that Section 5 should be used expansively to attack all manner of conduct a majority of the Commission perceives as bad for consumers
- Former Commissioner Rosch recently stated the FTC should challenge PAEs because “we have a gut feeling” they are anticompetitive.



Need for Limits on Section Still Exist

- Despite claims often made to the contrary, standalone Section 5 cases comprise a large portion of the FTC's enforcement agenda
- FTC brought four conduct cases this year; half were Section 5 enforcement actions



Need for Limits on Section Still Exist

- FTC claimed credit for consumer savings of roughly \$1 billion in FY 2012 from merger and non-merger enforcement actions
- Over 33% of these consumer savings are attributable to Section 5 standalone claims
 - 75% of consumer savings from FTC non-merger enforcement



Selecting a Principled Section 5 Standard

- Broad consensus in a number of key areas:
 - Most agree that Section 5 is broader than the traditional federal antitrust laws
 - Most agree that guidelines would be helpful, if not necessary, if the FTC uses Section 5 to reach conduct beyond the traditional antitrust laws
 - Most agree that one requirement of a Section 5 claim is showing “harm to competition”



Selecting a Principled Section 5 Standard

- Option 1: Standalone UMC violation requires evidence of a violation of the traditional federal antitrust laws
- Option 2: Standalone UMC violation requires evidence of harm to competition and no cognizable efficiencies



Selecting a Principled Section 5 Standard

- Option 3: Standalone UMC violation requires evidence of harm to competition and that the harms are disproportionate to any benefits
- Option 4: Standalone UMC violation requires evidence of harm to competition and that the harms outweigh the benefits



Selecting a Principled Section 5 Standard

- There are only minor differences between these four possible Section 5 standards:
 - Each requires showing “harm to competition”
 - Primary difference is how the Commission treats efficiencies in standalone Section 5 cases
- Question is which option will maximize the rate of return Section 5 cases earn consumers



Selecting a Principled Section 5 Standard

- Important to remember Section 5 has failed to date because FTC has sought to do too much and called into question whether any limits exist
- Commission must recalibrate Section 5 with eye towards regulatory humility to save the statute
- Wright Proposed Policy Statement does this by targeting Section 5 enforcement efforts at most plainly anticompetitive conduct—that without redeeming efficiency justifications



Thank you for your time.

