AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE FEDERAL TRADE COMMISSION AND ITS SECTION 5 AUTHORITY: PROSECUTOR, JUDGE, AND JURY

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JULY 24, 2014

Serial No. 113–142

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

90–892 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
DOC HASTINGS, Washington
CYNTHIA M. LUMMIS, Wyoming
ROB WOODALL, Georgia
THOMAS MASSIE, Kentucky
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
KERRY L. BENTIVOLIO, Michigan
RON DESANTIS, Florida

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
JACKIE SPEIER, California
MATTHEW A. CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
DANNY K. DAVIS, Illinois
PETER WELCH, Vermont
TONY CARDENAS, California
STEVEN A. HORSFORD, Nevada
MICHELLE LUJAN GRISHAM, New Mexico
Vacancy

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
STEPHEN CASTOR, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

	Page
Hearing held on July 24, 2014	1

WITNESSES

Mr. Michael Daugherty, Chief Executive Officer, LabMD, Inc.	
Oral Statement	7
Written Statement	10
Mr. David Roesler, Executive Director, Open Door	
Oral Statement	84
Written Statement	86
Mr. Gerald Stegmaier, Partner, Goodwin Procter	
Oral Statement	88
Written Statement	90
Mr. Woodrow Hartzog, Associate Professor, Samford University	
Oral Statement	122
Written Statement	124

THE FEDERAL TRADE COMMISSION AND ITS SECTION 5 AUTHORITY: PROSECUTOR, JUDGE, AND JURY

Thursday, July 24, 2014

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, D.C.

The committee met, pursuant to call, at 9:37 a.m., in Room 2154, Rayburn House Office Building, Hon. Darrell E. Issa [chairman of the committee] presiding.

Present: Representatives Issa, Mica, Turner, Duncan, Jordan, Chaffetz, Walberg, Lankford, Gosar, Massie, Collins, Meadows, Bentivolio, DeSantis, Cummings, Maloney, Norton, Tierney, Clay, Lynch, Connolly, Duckworth, Kelly and Lujan Grisham.

Staff Present: Jen Barblan, Senior Counsel; Molly Boyl, Deputy General Counsel and Parliamentarian; Ashley H. Callen, Deputy Chief Counsel for Investigations; Sharon Casey, Senior Assistant Clerk; Steve Castor, General Counsel; John Cuaderes, Deputy Staff Director; Adam P. Fromm, Director of Member Services and Committee Operations; Linda Good, Chief Clerk; Tyler Grimm, Senior Professional Staff Member; Christopher Hixon, Chief Counsel for Oversight; Mark D. Marin, Deputy Staff Director for Oversight; Ashok M. Pinto, Chief Counsel, Investigations; Andrew Shult, Deputy Digital Director; Rebecca Watkins, Communications Director; Jeff Wease, Chief Information Officer; Sang H. Yi, Professional Staff Member; Meghan Berroya, Minority Deputy Chief Counsel; Courtney Cochran, Minority Press Secretary; Jennifer Hoffman, Minority Communications Director; Julia Krieger, Minority New Media Press Secretary; Lucinda Lessley, Minority Policy Director; Juan McCullum, Minority Clerk; Dave Rapallo, Minority Staff Director; and Brandon Reavis, Minority Counsel/Policy Advisor.

Chairman ISSA. The committee will come to order. Without objection, the chair is authorized to declare a recess of the committee at any time. Today's hearing, "The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury."

The Oversight Committee mission statement is that we exist to secure two fundamental principles. First, Americans have a right to know that the money Washington takes from them is well spent. And second, Americans deserve an efficient, effective government that works for them. Our duty on the Oversight and Government Reform Committee is to protect these rights. Our solemn responsibility is to hold government accountable to taxpayers, because taxpayers have a right to know what they get from their government. It is our job to work tirelessly, in partnership with citizen watch-

dogs, to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy.

With that, I would recognize the ranking member for his opening statement.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Today's hearing will cover several new issues for this committee. First, the Republican briefing memo says that the committee will examine, "whether the FTC has the authority to pursue data security enforcement actions under its current Section 5 authority." In Section 5 of the FTC Act, Congress gave the FTC authority to protect American consumers, that is our constituents, and ensure that their personal, medical, financial, and other information is protected from unauthorized disclosure. The FTC has been using this authority to ensure that companies who receive this type of consumer information take appropriate steps to safeguard it. In fact, a Federal judge recently upheld this authority and rejected an attempt to, "carve out a data security exception."

Yesterday, Senator Rockefeller, the chairman of the Senate Commerce Committee and an expert on this issue, sent a letter to the chairman emphasizing this point. He wrote, "Another apparent purpose of your hearing is to express skepticism about the FTC's long-standing and well-established legal authority under Section 5 of the FTC Act. This skepticism is unfounded, and your public position was recently rejected by a Federal judge in the FTC data security case against Wyndham Corporation."

He goes on to say, "Over the past 13 years, the Commission has initiated dozens of administrative adjudicatory proceedings in cases in Federal court challenging practices that compromised security of consumers' data and that resulted in improper disclosures of personal information collected from consumers."

According to the Republican memo, today the committee will also examine, "recent FTC actions related to data security practices." One of the witnesses testifying today is Michael Daugherty, the CEO of a company called LabMD. The FTC has brought an enforcement action against LabMD, and Mr. Daugherty admits that more than 900 files on his billing manager's computer were accessible for public sharing and downloading, which is a major security breach.

Mr. Daugherty has written a book entitled "The Devil Inside the Beltway." In it, he refers to the FTC as, "terrorists," He also accuses the FTC of engaging in, "psychological warfare" and "torture," and of "administering government chemotherapy." Of course he has a right to his opinion, but this committee should base its oversight work on facts rather than the extreme rhetoric of a defendant in an ongoing enforcement action.

As part of our investigation, we have also received competing allegations about Tiversa, a data security firm that provided information to the FTC about LabMD's security breach. Obviously, we all agree that the FTC should rely only on evidence it believes to be legitimate. If allegations are ultimately verified that Tiversa provided intentionally falsified data, that data clearly should not be used in any enforcement action. But to date, we have obtained no evidence to corroborate these allegations. So they remain just that, unconfirmed allegations.

Unfortunately, on June 17th, the chairman sent a letter to the FTC inspector general alleging coordination and collaboration between the FTC and Tiversa, and suggesting that, "the FTC aided a company whose business practices allegedly involved disseminating false data about the nature of data security breaches." The chairman wrote that, "the FTC appears to have acted on information provided by Tiversa without verifying it in any meaningful way." He also requested that the inspector general examine the actions of several specific FTC employees.

I do not know how the chairman had reached these conclusions since the committee has not yet spoken to a single FTC employee. The committee just requested documents from the FTC less than a week ago, and the committee has obtained no evidence to support claims that the FTC officials directed Tiversa employees to fabricate information. To the contrary, every single current and former Tiversa employee interviewed by the committee staff has uniformly denied receiving any requests from FTC employees relating to fabricating information.

In response to the chairman's request for an investigation, the inspector general has now informed the committee that one of the employees named in his letter in fact was, "brought in to assist with the LabMD case after Tiversa was no longer involved, and she has not been working on the case for the past year." As I close, so it appears that some of the chairman's information was incorrect.

I am sure we will hear a lot of allegations today from parties in this ongoing litigation. Our job is not to take sides, but rather to serve as the neutral overseers and base our conclusions on the facts and the evidence.

The consequences of having personal information compromised can be devastating. As the new Republican majority leader Kevin McCarthy has said, "Nothing can turn a life upside down more quickly than identity theft." I agree with him. That is why I wrote to Chairman Issa in January proposing the committee examine the massive data security breach at Target, which may have compromised the personal information of more than 100 million American consumers. Instead of holding hearings like today's, which seeks to cast doubt on whether the FTC even has the authority to protect our constituents, the consumers, the American consumers, I hope the committee will turn to constructive efforts to improve corporate data security standards across the board. And I thank you, Mr. Chairman.

Chairman ISSA. I thank the ranking member.

Chairman ISSA. Today's hearing concerns the Federal Trade Commission and information this committee has uncovered that raises some important questions. As long as I have been chairman, and as long as I am chairman, this committee will focus, as its name implies, Government Oversight and Reform Committee. It is not for us to look first to the private sector. It is not for us to issue subpoenas and target private sector for their beliefs, for their practices, or for the failures that they certainly are paying a high price for, as Target is and should.

During my tenure, healthcare.gov was launched. Anyone of ordinary skill could have gone into the Web site, changed a few statements, a few of the letters in the top of the screen, while looking

at their record, and seen somebody else's record at the launch. On a billion-dollar Web design, it was vulnerable to ordinary hacking and accidents at the time it was launched.

The FTC did not sue President Obama or any of the chief information officers responsible for this failure. They did not sue the Secretary. They did not even sue the companies who delivered this shoddy work. Instead these were systematically, when discovered, corrected at taxpayers' expense. That was the right thing to do. When mistakes are made, when vulnerabilities are recognized, it's the responsibility of the entity to do its best to fix them.

If the Federal Trade Commission was overseeing companies whose vulnerabilities are exposed, demanding that they fix it or face the consequences, absolutely we would say they were doing their job. If the Federal Trade Commission had even published a best practices minimum requirement for data security, we would be able to say that the law was clear, and that somebody failed to live up to those stated guidelines. But none of these exist. The Federal Trade Commission cannot tell you what is right; they only will come in and demand a consent decree if, in fact, you, through fault or no fault of your own, become a victim of hacking or a recognition of a vulnerability.

The FTC is using its regulatory authority not to help protect consumers, but, in fact, to get simple consent decrees using the unlimited power it has to not only sue at government expense, but to force you before administrative law judges that, in fact, are part of the executive branch. Millions of dollars will be spent attempting to defend yourself against the Federal Trade Commission even if you are right. And what if you're wrong? What if you're wrong? What if something happened? What is your choice?

Several years ago, under Chairman Waxman, I watched a demonstration of a vulnerability created by a third-party software that people were using to share music. I'm a techie. I was impressed. I saw that this software was downloaded by hundreds of thousands of people, put onto computers they owned or didn't own, and it created a vulnerability. It was deceptive—at least according to testimony, it was deceptive in how it did it. And our own people loaded the software and agreed that when you loaded it, the default would make the hard drive of the computer it was loaded on vulnerable in every one of its directories, when, in fact, you were really only attempting to make your music directory available for sharing.

In both public and private systems around the country, this software was downloaded and created what people thought was a peer-to-peer music sharing, and, in fact, created a vulnerability in which people could look at what was on your hard drive.

We were aghast. We thanked our witnesses for making us aware of it, and we committed ourselves to stop the deceptive practice of this software company, something over which the FTC had authority and should have acted.

But, in fact, what we are finding is that what we were told was only a part of the story. When information does—the question today is how is the FTC using that regulatory authority, and are they doing their job? Are they targeting the culprit or the victim? What information does the agency consider to be a reliable basis to embark?

Mr. LYNCH. Mr. Chairman, could I ask you why the clock is not running on any of this?

Chairman ISSA. We didn't stop the ranking member from going as long as he wanted, well over the time. That's the practice of the committee. I thank you.

Mr. LYNCH. That's a good answer. Thank you.

Chairman ISSA. What information does the agency consider to be a reliable basis to embark on often erroneous inquisitions, in the chairman's opinion, into the activities of American companies?

The committee held two hearings in the past, as I mentioned, one in 2007 and another in 2009, about the potential for individuals using peer-to-peer file-sharing programs to inadvertently share sensitive or otherwise confidential information. The key witness in both of these hearings was Mr. Robert Boback, the CEO of a cyber intelligence firm, Tiversa, Incorporated. That CEO outlined numerous data breaches that deeply troubled members of the committee.

Mr. Boback specifically spoke about an Open Door Clinic, a nonprofit AIDS clinic in Chicago's suburbs in 2009. He said, "These are AIDS victims, 184 patients, who are now victims of identity theft. The clinic released their information and has not addressed it." But the Open Door Clinic has told us they have no information of any of their patients having had their identities stolen. We do not know why Mr. Boback made the claim to this committee previously, and we will hear that today.

Earlier this year this committee became aware, on a bipartisan basis, of serious accusations that Tiversa engaged in a business model that was not focused on protecting consumers alone, but obtaining what we would say effectively is a new form of protection payments from businesses. As is often the case with protection payment demands, many businesses that did not pay up faced serious consequences.

Here's how it worked. Tiversa would contact a company or organization and tell them that they had engaged in a practice that left customers' data vulnerable. Tiversa would offer to sell the company or organization remediation services. Many companies took their services and paid, at least for a while. Others refused and found themselves turned over to the Federal Trade Commission.

The cost and concerns created by an FTC investigation can be immense, particularly to a small business that in many cases were the ones that Tiversa focused on. But this isn't just about allegations of unethical corporate behavior. The committee has asked the Federal Trade Commission to provide us with evidence that it independently verified information provided by Tiversa about businesses before pursuing action. As the ranking member said, it's been a short time, but having engaged in suits, received consent decrees, and litigated for years, we expected that the Federal Trade Commission would be able to give us at least a few examples of independent confirmation immediately. We are still waiting for the FTC to show us such evidence. We look forward to it. And as I will say again, we look forward to hearing from the FTC in the future directly.

It's one thing for a company like Tiversa to report all of its concerns about consumer data breaches to appropriate authorities. It's

quite another when enforcement authorities are selectively used, through a special relationship, to punish firms who refuse to pay for those services.

The committee has reason to believe that information provided by Tiversa on which the FTC relied was inaccurate. Two of our witnesses this morning were approached by Tiversa and the FTC regarding data breaches. Tiversa provided information that alleged data breaches in these organizations to—about these breaches in these organizations to the FTC only after they refused to sign up for Tiversa's services.

Mr. Daugherty, the CEO of LabMD, according to my opening statement, has been to hell and back. I don't think he's gotten back yet. In fact, his fight with the FTC has gone on for years. The Commission wanted him to acquiesce to a consent decree admitting that he did not take proper precautions to avoid data breaches.

Given that Mr. Daugherty did not believe the allegations against him were true or fair, he fought back, and he did so at great personal expense. His specialized cancer-screening company is now effectively nonexistent.

I will let Mr. Roesler explain his experience with Tiversa and the tribulations he experienced thereafter, but I especially want to thank him for being here today. Mr. Roesler runs, as previously mentioned, a nonprofit AIDS clinic near Chicago, Illinois, and has taken time away from his important work and agreed to join us this morning because of how important he believes it is to tell his story.

I also want to thank Mr. Stegmaier for appearing this morning. He will be providing invaluable testimony about the FTC's actions as they relate to going after companies that are alleged to have unfair, deceptive trade practices.

Today's hearing is an opportunity to hear from alleged victims of these arrangements made between Tiversa and the Federal Trade Commission. Neither the FTC nor Tiversa are here today, but I do expect to have both of them here at a future date to respond to the concerns and allegations that I expect we will hear today.

Today's hearing is the result of a whistleblower who at great personal expense came to this committee. This committee is grateful to all the brave individuals who come forward to provide information as whistleblowers. It is only through whistleblowers that we see an exposure of wrongdoing by the government as well as private companies. Whistleblowers are not always without responsibility. Whistleblowers may, in fact, know what they know because for a time they participated in the wrongdoing. Nevertheless, whistleblowers are invaluable. When someone's conscience, whether they were involved or not, brings them forward, they should never be the target of this committee.

This whistleblower gave us a proffer, seeking immunity only for what he was to testify to that he had done on behalf of Tiversa. He detailed for this committee information that was invaluable to our ongoing—to our investigation, which is only ongoing because of his coming forward.

At a point in the future, I expect this committee will need to schedule a vote on granting immunity for this whistleblower. To date, we have not been able to convince the minority to consider

immunity for this whistleblower. Instead, at every turn the minority has chosen to seek accusations against the whistleblower; against his personal wrongdoing, his personal misconduct, his personal life. But, in fact, to our knowledge, no evidence has come forward that would in any way dispute the accuracy of the detailed story that he told.

For those Members here on both sides of the aisle, if you have not already seen his video proffer of how he participated in the activity, I ask you to schedule time, Members only, to see this proffer, because as we consider immunity, it is important that you understand the nature and detail of the evidence and accusations brought by this whistleblower.

I make no credible statement as to a whistleblower's authenticity. What I can say in this case is without the whistleblower, we would not be having this hearing today. And if the whistleblower is guilty of a crime, the crime had to be committed by others that he is accusing. There can be no crime if, in fact, he is not telling the truth. And if he is telling the truth, he participated in a deception that affected both the Federal Trade Commission and the United States Congress.

I would ask all Members, please, take time out of your busy schedule to view the proffer. It is detailed, it takes nearly an hour, but it will lead, I believe, to the kind of recognition that you cannot see here today in an open hearing.

Chairman ISSA. It is now my honor to welcome our witnesses. Mr. Michael Daugherty is the chief executive officer of LabMD. Mr. David Roesler is executive director of Open Door Clinic in Illinois. Mr. Gregory Stegmaier is a partner at Goodwin Procter in D.C., in Washington, D.C. And Mr. Woodrow N. Hartzog is an associate professor at the Cumberland School of Law at Samford University.

Gentlemen, pursuant to the committee rules, would you please rise to take the oath and raise your right hand?

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Please be seated.

Let the record indicate that all witnesses answered in the affirmative.

For our first two witnesses in particular, you are here to tell your story. I know testimony is new to you. We have a 5-minute rule. Your entire opening statements as prepared will be placed in the record. But I understand that you may go over slightly. We are not going to hold you exactly to 5 minutes, but to the greatest extent possible, try to stay within the 5 minutes, which will help us ask you more questions in follow-up dialogue.

Mr. Daugherty.

WITNESS STATEMENTS

STATEMENT OF MICHAEL DAUGHERTY

Mr. DAUGHERTY. Thank you.

Good morning, Chairman Issa, Ranking Member Cummings, and members of the committee. My name is Michael Daugherty, and I am the president and CEO of LabMD, 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 40 medical professionals who touched nearly 1 million lives. Thank you for the opportunity to speak to you as a small businessman and medical professional about my experience and opinion at the hands of the Federal Trade Commission.

What happened to my company, its employees, physicians, and their patients is what springs from the FTC's unsupervised playbook, and that playbook relies upon coercive and extortionist strategies to make large and small companies alike quickly succumb to FTC demands.

In May 2008, our nightmare began with a call that could happen to any American. It was from Robert Boback, the CEO of Tiversa. And in the words of former FTC Commissioner Rosch, Tiversa is more than an ordinary witness, informant, or whistleblower. It is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks.

Mr. Boback told LabMD that Tiversa had found LabMD patient data on the Internet, but refused to tell us more unless we paid and retained them. Everyone in medicine knows you cannot go out intentionally looking for vulnerable medical files so you can take them, read them, keep them, distribute them. This is probably a crime, but it's definitely vigilante behavior, and it's outrageous.

In January of 2010, Alain Sheer, an attorney with the FTC, contacted LabMD with an 11-page, single-spaced letter opening a nonpublic inquiry. We responded by sending in nearly 10,000 pages of documents, and we invited the FTC to come to Atlanta to see our facility, to tell us what to do differently, to tell us what their standards were. 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.

When we asked the FTC where they were going with this, they would obscurely mention consent decrees, and we learned that FTC consent decrees actually are this: You sign up for 20 years of audits, you enter the FTC "hall of shame" via craftily worded press releases and half-truth congressional testimony. The fact that you have not been found any wrongdoing stays buried deep in the fine print. And the threat of being tied up for years in court and drained financially is their gun to the head to extract false confessions.

In August 2010, I had to find out what was going on here, because something felt odd and wrong. And I learned that Homeland Security gave $24 million to Dartmouth to partially fund their data hemorrhage study. And Dartmouth stated that it got the LabMD file by using Tiversa's unique and powerful technology.

Tiversa put out a press release in May 2009 I found, which in part stated, Tiversa—this is their words—"Tiversa today announced the findings of new research that revealed 13 million breached files emanating from over 4 million sources. Tiversa's patent-pending technology monitors over 450 million users, issuing 1.5 billion searches per day. Over a 2-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; a 1,718-page document from a medical testing labora-

tory. And requiring no software or hardware, Tiversa detects, locates, and identifies exposed files in real time."

What does Tiversa want you to think "exposed" means? Out of 13 million files found by Tiversa, how odd is it that the 2 mentioned in their press release are sitting at this table today?

I was stunned that nobody was asking who this private company was who was stockpiling other people's sensitive information. What gave them the right to assume ownership?

September 2013 to April 2014, the FTC pursued litigation against LabMD via their optional administrative process rather than in Federal court. FTC Commissioner Wright said this process provides the FTC with institutional and procedural advantages. This is lawyerspeak for the FTC stacks the deck way in favor via rules Congress allows them to make. They admit hearsay that would never fly in Federal court, which is why we aren't in Federal court. Federal courts won't intervene because Congress says they can't.

When asked about the FTC data security standards, Alain Sheer said, "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 show others what happens if you push back. They subpoenaed approximately 40 different individuals from my company, long-gone LabMD employees that left the company up to 7 years before, current staff, managers, outside physicians, vendors. These witnesses were forced to retain counsel and were intimidated and scared. Here is the message to all that are watching from the FTC: This is FTC justice, and this is going to happen to you if you don't play along.

And then the penny dropped. During the trial, a former Tiversa employee who was to testify regarding Tiversa's acquisition of LabMD data and subsequent submission of the data to the FTC invoked his Fifth Amendment right against self-incrimination.

All Americans should be outraged by the FTC's unchecked ability to pursue a claim that is not based on 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. If this has happened to LabMD, a small medical facility, a cancer-detection center, this can happen to anyone.

This does nothing to help Americans adapt to the constantly changing cybersecurity landscape. We are not mind readers; we are law-abiding citizens. I call on the FTC to stop attacking victims of crimes. And I thank the committee for its time and attention to this matter.

Chairman ISSA. Thank you.

[Prepared statement of Mr. Daugherty follows:]

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

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 E. 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-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 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

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

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

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.

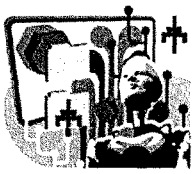
Best Regards,

Stephen F. Fusco
General Counsel

cc: Philippa V. Ellis, Esq.

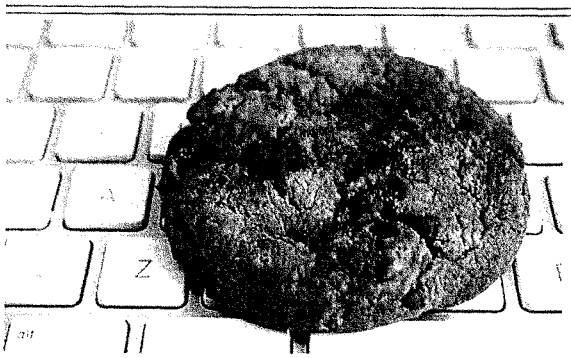
theguardian

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 mamjority 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.

Zip file

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 (Bilibr)

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@tiversa.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@tiversa.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 practioners (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 your 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 Keevan — 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 micromanage 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." ○

This editorial series has been developed in cooperation with Morgan, Lewis & Bockius LLP.

PRWeb

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

PRWeb®

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.

###

If you have any questions regarding information in these press releases please contact the company listed in the press release. Our complete disclaimer appears here. - PRWeb ebooks - Another online visibility tool from PRWeb

PRWeb

Contact Information
Scott Harrer
Tiversa
http://www.tiversa.com
724-940-9030

Online Web 2.0 Version
You can read the online version of this press release here.

If you have any questions regarding information in these press releases please contact the company listed in the press release. Our complete disclaimer appears here. - PRWeb ebooks - Another online visibility tool from PRWeb

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 Wikileak'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: asheer@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 *insurancuaging_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 though 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); websites; 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-REGFAIR (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.

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.

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 other-wise oppressive, and do so without a justification that is grounded in legitimate, independent self-interest. (emphasis added)

-- Former Chairman Jon Leibowitz (2006)

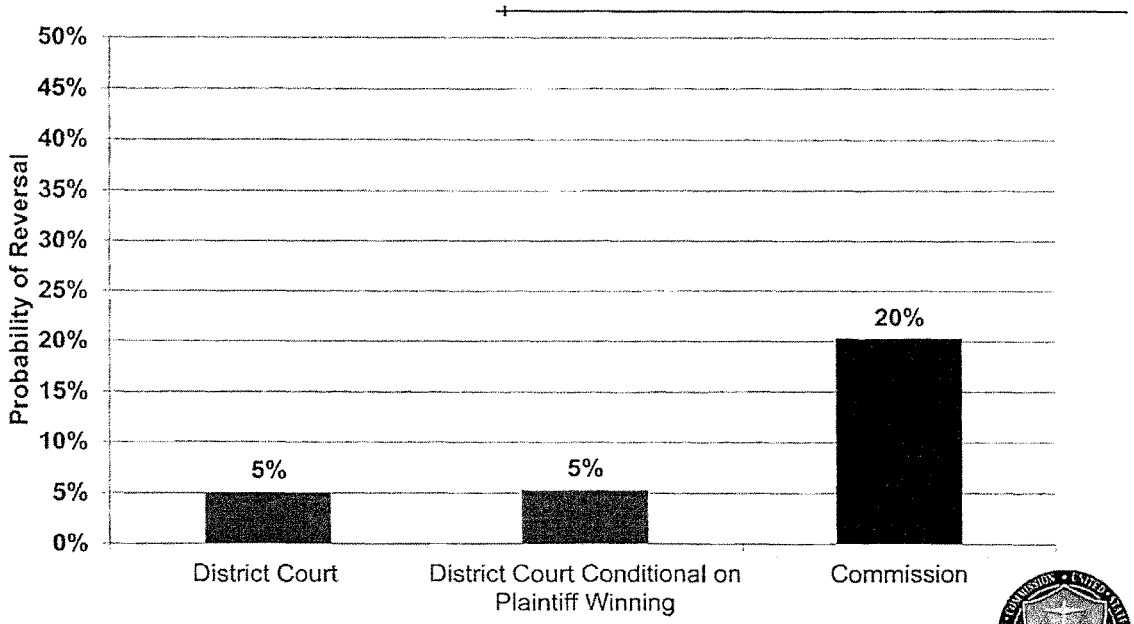
Identifying the Section 5 Problem

- 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.

Chairman ISSA. Mr. Roesler.
I'm sorry, you're finished, right?
Mr. DAUGHERTY. Oh, yeah.
Chairman ISSA. Thank you.
Mr. Roesler.

STATEMENT OF DAVID ROESLER

Mr. ROESLER. Good morning, committee members. My name is David Roesler. I am and have been the executive director of Open Door Clinic in Elgin, Illinois, the far western suburbs of Chicago, for the past 15 years. I am appearing today in response to an invitation to testify on behalf of Open Door regarding its involvement with the FTC and a company called Tiversa.

Between September of 2008 and March of 2013, Open Door was involved in a class-action lawsuit due to a file that was found on the Internet that contained names, some with Social Security numbers, some with addresses, some with birth dates.

Open Door is a small, not-for-profit AIDS organization. Currently we have about 30 employees. We had about 15 during this time. We provide medical care, support services for our clients.

In July of 2008, a company called Tiversa contacted Open Door and said that they had had access to a confidential document obtained from a P2P network on the Internet. Communications with Tiversa included a contract for services. The suggested fees for the contract were $475 an hour. We contacted our IT service provider, who researched our network; found no evidence of any P2P networks at that time.

In September of 2009, Tiversa contacted Open Door again to report that documents were still available on the P2P software. Open Door's IT provider once again reviewed its network to confirm that there was no evidence of any P2P software at that time.

Two months after that, in November of 2009, clients began calling their case managers at the clinic, reporting that they were receiving phone calls from a law firm asking them to join a class-action lawsuit because their information had been released by Open Door. At Open Door's November board meeting, shortly after the clients started calling, one of the board members is a client. He brought in a letter that he got in the mail, also from this out-of-State law firm, telling them that they had their information out on the Internet, and would they join a class-action lawsuit.

Then in January of 2010, we received a letter from the FTC. The letter indicated that they had found a file on a peer-to-peer network, and it had a different title than the document that had been reported found by Tiversa.

Also in January that same month, in 2010, Open Door was successful at getting a law firm to provide us some pro bono work to help us understand what our compliance and responsibilities were. Open Door and its IT provider once again reviewed our network, all of our workstations to confirm that there was no P2P software at that time.

In February, a month later, February of 2010, a class-action lawsuit was filed in Kane County against Open Door. Sensational newspaper headlines; numerous media outlets began showing up at our door. And 3 years later Open Door's settlement agreement was

approved by the court, dismissing the class action. Open Door and its insurers agreed to these motions.

Open Door denied, and continues to deny, any legal responsibility for the disclosure. Had the case been tried, we would have expected to prevail, but because of the uncertainties, the expense of litigation, Open Door and its insurers agreed to terminate this litigation under these terms.

Thank you for letting me tell my story.

Chairman ISSA. Thank you.

[Prepared statement of Mr. Roesler follows:]

Testimony for the House Committee on Oversight and Government Reform

Good Morning Committee Members,

My name is David Roesler and I have been the Executive Director of Open Door Clinic of Greater Elgin for the past 15 years.

I am appearing today in response to an invitation to testify on behalf of Open Door regarding its involvement with the FTC and a company called Tiversa.

Between September 2008 and March 2013, Open Door was involved in a class action lawsuit due to a file that was found on the internet that contained names, some with social security numbers and some with addresses and birthdates.

Open Door is a small not-for-profit AIDS Service Organization, approximately 30 employees, providing medical and support care for people living with HIV/AIDS in the far western suburbs of Chicago Illinois.

In July 2008 a company called Tiversa contacted Open Door and said that they had access to a confidential document obtained from a P2P network on the Internet.
Communications with Tiversa included a contract for services. The suggested fees for the contract were for $475/hr.

We contacted our IT Service Provider who researched our network and found no evidence of any P2P networks at that time.

In September 2009, Tiversa contacted Open Door again to report that documents were still available on P2P software.

Open Door's IT Service Provider, once again, reviewed its network to confirm that there was no evidence of P2P software.

Nov 2009 clients began calling their case workers reporting that they were receiving phone calls from lawyers asking them to join a class action lawsuit due to their information released by open door.

At Open Door's November Board Meeting, one board member, also a client, brought in a letter from an out of state law firm asking them to join a class action lawsuit.

January 2010, we received a letter from the FTC. The letter indicated that they had found a file on a P2P Network with a different title than that revealed by Tiversa.

Also in January 2010, Open Door was successful in getting an engagement letter with a law firm to provide pro bono services and began to review our responsibilities of compliance.

Open Door and its IT provider once again reviewed our network and each workstation to confirm that there was no P2P software at that time.

February 2010, a class action lawsuit was filed in Kane County Illinois against Open Door.

Sensational newspaper headlines and numerous media outlets began calling and showing up at the clinic.

March 7, 2013 Open Door's Settlement agreement was approved by court order, dismissing the class action.

Open Door and its insurers agreed to these motions. Open Door denied and continues to deny any legal responsibility for the disclosure, had the case been tried we would've expected to prevail but because of the uncertainties and expense of litigation Open Door and its insurers agreed to terminate this litigation under these terms.

Chairman ISSA. Mr. Stegmaier.

STATEMENT OF GERARD M. STEGMAIER

Mr. STEGMAIER. Mr. Chairman Issa, Ranking Member Cummings, members of the subcommittee, my name is Gerry Stegmaier, and I'm pleased to be here today to discuss the Federal Trade Commission's data security enforcement activities under Section 5 of the FTC Act. The views I express are my own, not of our clients or of our firm.

I'm a partner at Goodwin Procter LLP, and an adjunct professor at George Mason University School of Law, where I've taught privacy, consumer protection, and constitutional law courses for the last 13 years. I regularly appear before the Federal Trade Commission, State attorneys general, and assist businesses with all aspects of their privacy and information governance concerns. I appreciate the opportunity to appear before you today.

In 2013, there were 63,437 reported security incidents, and 1,367 confirmed data breaches. That is not a number reporting the number of accessible information, which is one of the things that Mike spoke about. According to Verizon's 2014 data breach investigation report, 44 million data records across the globe have been exposed.

Companies are aware of the need for data security, and have taken steps to be more secure. Data security is important to consumers, the economy, and business, but equally important is the basic constitutional principle that people have a right to know what the law expects of them before we prosecute them.

I think a simple analogy helps illustrate this in practice. When we want people to regulate how fast they drive their cars, we post speed limit signs. If you violate that posted limit, and the sign has been there for more than 60 days, you will likely receive a citation. The law calls this fair notice, and the Constitution protects us from government overreach with it. It is the shield that protects us from the deference that agencies receive.

While this analogy may not be a good one, it's important to note that it represents the feelings of many organizations that confront FTC enforcement actions relating to data security.

The agency has offered no formal rulemakings or adjudications related to data security, and the FTC appears to regulate data security primarily through complaints and consent orders, as we've heard. Neither the complaints nor the consent orders are binding, reliable precedent. They are nonprecedential. Some might call this stop-and-frisk black box justice.

FTC complaints and consent orders are inconsistent and often lack critical information. For example, it is often unclear whether implementing some or all of the measures in a given order would result in fair data security, or even serve to avoid future enforcement actions had the underlying company admitted them in the first instance or practiced them.

The FTC's often repeated position is that security standards can't be enforced in an industry-specific, case-by-case manner without more guidance provides little comfort to those appearing before the agency. Because the FTC decides on an individual and postinfraction basis whether a company is noncompliant, the risk of enforcement actions is unimaginable and unpredictable, as we

have heard. The penalties that may result from noncompliance are potentially ruinous. Combined with ambiguity of the law, unnecessary compliance risks for regulated entities has created a situation ripe for overreach, unfairness, and an uneven application of the law.

The FTC's existing enforcement and guidance practices also pose serious due process concerns relating to fair notice of the law's requirements. Current enforcement environment consists of aggressive enforcement against the victims of third-party criminal hacking who operate in a realm without clear and unmistakable data security law. Improved authoritative—and I emphasize authoritative— interpretations of Section 5 by the agency and the courts are crucial to improve compliance and provide entities with sufficient information to understand how to respond.

Let me be clear. The FTC has the means to more clearly define the law and provide useful, reliable guidance. The existing tools are there. Sadly, there's plenty of room for improvement with the use of these existing tools, and improvements are essential to clarify the underlying uncertainty, which we have heard about, and, more importantly, to address the constitutional issue of fair notice and due process.

The current reasonableness test, absent additional flexible, principles-based authoritative guidelines or court-resolved litigation, will do little or nothing to clarify the data security obligations of companies. Using the standards reasonable and appropriate without articulating such factors as the nature of business, the kind of information collected, or any other factors that may come into play may not ensure that fair notice occurs.

In essence, we tell our clients do what you say and say what you do. We need to hear from the agency what they're doing and what they're saying so that the people who are subject to prosecution can understand how to respond and how to behave in the first instance.

The FTC itself has not consistently defined what sensitive information is, and without clarification, the agency's enforcement will continue to be perceived as arbitrary, and we will lack an understanding of reasonableness.

I thank you for your time and attention. I'm pleased to answer any questions you might have.

Chairman ISSA. Thank you.

[Prepared statement of Mr. Stegmaier follows:]

Prepared Statement of

Gerard M. Stegmaier
Partner, Goodwin Procter LLP
Adjunct Professor, George Mason University School of Law

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

Before the

Committee on Oversight & Government Reform
United States House of Representatives

Washington, D.C.
July 24, 2014

Mr. Chairman Issa, Ranking Member Cummings, and Members of the Subcommittee, my name is Gerry Stegmaier, and I am a partner at Goodwin Procter LLP and an adjunct professor at George Mason University School of Law, where I created one of the first information privacy law courses and have taught courses relating to privacy, consumer protection, and constitutional law for the last 13 years. I regularly appear before the Federal Trade Commission and state attorneys general, and I assist businesses with all aspects of their privacy and information governance concerns. I appreciate the opportunity to appear before you today to talk about the Federal Trade Commission's data security enforcement efforts under Section 5 of the Federal Trade Commission Act.[1]

INTRODUCTION

In 2013, there were 63,437 reported security incidents and 1,367 confirmed data breaches affecting more than 44 million data records across the globe according to Verizon's 2014 Data Breach Investigation Report.[2] Most data breaches involve malicious criminal activity stemming from outsiders.

While entities have business incentives to protect the information they collect, there is no single broad federal law requiring data security. Instead, the law has focused on criminalizing unauthorized access. This is not surprising since the law generally favors open and broad accessibility of information. Congress has limited its data-security legislation to certain industries, such as finance and healthcare, where public debate led to a consensus that increased information protection legislation was required. Generally, in the United States, data stewardship

---

[1] The views contained in this testimony solely represent the views of myself in my individual and private capacity and are not necessarily the views of my firm, our clients, or any particular institution with whom I may be affiliated.
[2] *2014 Data Breach Investigations Report*, VERIZON, 11, *http://www.verizonenterprise.com/DBIR/2014/* (last visited July 21, 2014).

is encouraged primarily by state-enacted breach notification requirements.[3]

Over the last decade, the FTC has begun requiring reasonable data security for entities not covered by existing, industry-specific federal regulations. The FTC routinely investigates publicly reported data-related incidents and has brought more than 40 data-security cases since 2000.[4] The FTC has become increasingly aggressive, as demonstrated by an FTC consent order with HTC America after the company's mobile security vulnerabilities allegedly *potentially* exposed sensitive information, even though no *actual* data compromise was alleged.

The FTC bases its authority over data security on § 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[5] Usually, the FTC makes a deceptive practices claim when an entity experiences a data breach after publishing statements that it secures data.[6] Less frequently, the FTC alleges unfair practices in data-security cases.[7] However, § 5 does not mention data security, which begs a practical question: Because the Constitution requires that entities receive fair notice to reasonably understand what behavior complies with the law, does the investigation and prosecution of entities under § 5 in data-security cases violate entities' constitutional rights to fair notice? And. if so, how might these due process concerns be better addressed?

While the Fair Notice Doctrine began in the context of criminal defense, in 1968 the U. Court of Appeals for the District of Columbia Circuit acknowledged the doctrine's applicability

---

[3] Notably, some states, such as California, have data-security requirements. *E.g.*, CAL. CIV. CODE § 1798.81.5(b) (West 2006) ("A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.").
[4] *See* Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 13, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-CV-01887-ES-SCM (D. N.J. June 17, 2013) [hereinafter Wyndham FTC Response].
[5] 15 U.S.C. § 45 (a)(1) (2006).
[6] Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 7, *FTC v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012).
[7] *Id.* (stating that seventeen of the thirty-six cases brought under the FTC Act alleged unfair practices).

in the civil administrative context.[8] The court observed, "Where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property by imposing civil or criminal liability."[9]

The fair notice doctrine is not a trivial, academic legal theory with little bearing on the practice of law. On the contrary, given the FTC's broad discretion under § 5 of the FTC Act, the FTC's aggressive enforcement stance in the data-security context, and the agency's reluctance to use its existing rulemaking authority to clarify its data-security expectations, the doctrine is directly relevant to the current regulatory climate.[10] Although the FTC has undertaken significant efforts to develop and improve notice of its interpretation of § 5, the nature, format, and content of the agency's data security-related pronouncements raise equitable considerations that create serious due process concerns.[11]

FAIR NOTICE DOCTRINE

WHAT IS THE FAIR NOTICE DOCTRINE?

The fair notice doctrine requires that entities be able to reasonably understand whether their behavior complies with the law. If an entity acting in good faith cannot identify with "ascertainable certainty" the standards to which an agency expects it to conform, the agency has not provided fair notice.[12] An agency using enforcement conduct, rather than less adversarial methods, to define the contours of its broad discretion likely raises greater due process

---

[8] *Radio Athens, Inc. v. FCC*, 401 F.2d 398, 404 (D.C. Cir. 1968).
[9] *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995).
[10] Fair notice is particularly important when courts defer to an agency's interpretation of the scope of its jurisdictional authority. When agencies may define the breadth of their authority under broadly-worded statutes, fair notice may be one of few constraints on arbitrary and capricious agency action. For example, in *City of Arlington v. FCC*, the Supreme Court reviewed the FCC's assertion of jurisdiction under the Communications Act over applications for wireless facilities. The Supreme Court concluded that a court should defer to any agency's interpretations of the statute that it enforces, even those regarding the extent of the agency's authority. *City of Arlington, Texas v. FCC*, 596 U.S. ___, 133 S. Ct. 1863 (2013).
[11] In its response to Wyndham's motion to dismiss, the FTC stated, "unreasonable data security practices are unfair." *See* Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 7, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-CV-01887-ES-SCM (D. N.J June 17, 2013). The FTC argues that Wyndham has notice from government and industry sources about what security practices are reasonable.
[12] *Gen. Elec.*, 53 F.3d at 1329 (citing *Diamond Roofing Co. v. OSHRC*, 528 F.2d 645, 649 (5th Cir. 1976)).

concerns.[13] Due process protections, like those provided by the fair notice doctrine, increase in importance in these circumstances. A defendant may raise the fair notice defense to defend itself against agency enforcement when it feels it has not received proper notice.[14]

DISTINCTION BETWEEN *CHEVRON* DEFERENCE AND THE FAIR NOTICE DOCTRINE

The fair notice doctrine can serve as an effective defense even when a statute passes *Chevron* deference. *Chevron* deference is a powerful legal doctrine based on the assumption that federal agencies are experts on the statutes they enforce.[15] Under *Chevron*, courts defer to agencies' reasonable interpretations of the statutes they enforce when such statutes are ambiguous.[16] However, if an agency interpretation is unpublished or unclear, entities can argue that an agency should not hold them accountable for noncompliance under the fair notice doctrine and if such an argument prevails, the court will dismiss the claims stemming from that interpretation, or lack thereof.

THE FAIR NOTICE TEST AS APPLIED BY THE D.C. CIRCUIT

The fair notice doctrine is a creature of judicial creation not yet reviewed or bounded by

---

[13] *See e.g.*, *Martin v. OSHRC*, 499 U.S. 144, 158 (1991) (citing *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 295 (1974)) ("[T]he decision [by an agency] to use a citation as the initial means for announcing a particular interpretation may bear on the adequacy of notice to regulated parties.").

[14] *See* Kenneth K. Kilbert & Christian J. Helbling, *Interpreting Regulations in Environmental Enforcement Cases: Where Agency Deference and Fair Notice Collide*, 17 VA. ENVTL. L.J. 449, 454 (1998) ("The fair notice principle mandates that persons may not be punished for failing to comply with a law of which they could not have known."); Albert C. Lin, *Refining Fair Notice Doctrine: What Notice Is Required of Civil Regulations?*, 55 BAYLOR L. REV. 991, 998 (2003) ("[D]ue process requires . . . that parties subject to administrative sanctions are entitled to fair notice because civil penalties result in a deprivation of property . . . ."); John F. Manning, *Constitutional Structure and Judicial Deference to Agency Interpretations of Agency Rules*, 96 COLUM. L. REV. 612, 669-70 (1996) ("[I]t is arbitrary and capricious for the government to deny benefits based on noncompliance with standards that a putative beneficiary could not reasonably have anticipated."); Jeremy Waldron, *Vagueness in Law and Language: Some Philosophical Issues*, 82 CALIF. L. REV. 509, 538 (1994) (describing the unfairness of imposing vague legal requirements); Jason Nichols, Note, *"Sorry! What the Regulation* Really *Means Is...": Administrative Agencies' Ability to Alter an Existing Regulatory Landscape Through Reinterpretation of Rules*, 80 TEX. L. REV. 953, 964 (2002) ("Armed with knowledge of the bounds of acceptable action, people will be better able to plan their actions and will know when the government unjustly trounces upon their liberties.").

[15] *Gen. Elec.*, 53 F.3d at 1327 (citing *Chevron, U.S.A., Inc. v. Natural Res. Def. Council*, 467 U.S. 837, 864-66 (1984)). For more information on *Chevron* deference, *see* Kristine Cordier Karnezis, Annotation, *Construction and Application of "Chevron Deference" to Administrative Action by United States Supreme Court*, 3 A.L.R. Fed. 2d 25, 39 (2005); 2 AM. JUR. 2d *Administrative Law* § 77 (2002).

[16] *Chevron, U.S.A., Inc. v. Natural Res. Def. Council*, 467 U.S. 837, 864-66 (1984); *Gen. Elec.*, 53 F.3d at 1327.

the Supreme Court. The D.C. Circuit, the federal appeals court most frequently confronted with important questions of administrative law, has the most developed fair notice jurisprudence.

"Ascertainable Certainty": The D.C. Circuit's Test

In a nutshell, fair notice requires that a party be able to determine an agency's expectations with "ascertainable certainty" in order to satisfy due process requirements. Fair notice exists when "a regulated party acting in good faith would be able to identify, with 'ascertainable certainty,' the standards with which the agency expects parties to conform."[17] "The regulations and other public statements issued by the agency"[18] should provide this ascertainable certainty.

What is "Ascertainable Certainty"?

The words "ascertainable certainty" are not particularly clear; four factors have been identified to apply the standard by the D.C. Circuit:

1. ***Does the Plain Text of the Law Provide Notice, and Is the Regulated Entity's Interpretation Plausible?***

The D.C. Circuit has held that the most important factor for a successful fair notice defense is whether a careful reading of the law's plain language provides the necessary notice of the law's meaning.[19] "[W]here the regulation is not sufficiently clear to warn a party about what is expected of it"[20] the fair notice doctrine protects a party from government sanction. The language of the regulation provides proper notice only if it is "reasonably comprehensible to people of good faith."[21] Where the law is silent or ambiguous and multiple interpretations exist,

---

[17] *Gen. Elec.*, 53 F.3d at 1329 (citing *Diamond Roofing*, 528 F.2d at 649).
[18] *Id.* (citing *Diamond Roofing*, 528 F.2d at 649).
[19] *See McElroy Elecs. Corp. v. FCC*, 990 F.2d 1351, 1353, 1362 (D.C. Cir. 1993).
[20] *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1328 (D.C. Cir. 1995).
[21] *Id.* at 1330-31 (quoting *McElroy Elecs.*, 990 F.2d at 1358).

the D.C. Circuit has applied the fair notice doctrine to protect parties from government sanctions.

2. *Do "Authoritative" Pre-Enforcement Efforts by the Agency, Such as Public Statements, Provide Adequate Notice?*

Courts will determine whether the conduct of the agency ensures adequate notice by reviewing the agency's public statements and actions, such as notices published in the Federal Register,[22] adjudicatory opinions,[23] previous citations,[24] and policy statements. To my knowledge, the D.C. Circuit has not analyzed whether a single-party consent decree or settlement with an agency constitutes a reviewable and authoritative interpretive document as part of the "ascertainable certainty" test.

Moreover, to meet fair notice requirements, agency guidance must be "authoritative" and originate from the agency as a whole.[25] Statements from some other source, like the opinion of agency staff or even a single commissioner who may not be speaking for the entire agency, are insufficient.[26] A court would need to determine whether an agency's public statements, such as published complaints, consent orders, and guidance came from the agency as a whole. If they did not, a court should not consider them as a source of notice. Regulated entities should be able to clearly determine which statements identify the law's requirements, and which do not. By limiting the authoritative source to agencies as a whole, courts relieve regulated entities from

---

[22] *See Darrell Andrews Trucking, Inc. v. FMCSA*, 296 F.3d 1120, 1130-32 (D.C. Cir. 2002) (concluding that the formal regulatory guidance and notice of proposed rulemaking published in the Federal Register were self-contradictory); *Chrysler Corp.*, 158 F.3d at 1356 (reviewing the Federal Register notice discussing the rule and concluding that the notice was silent on the matter).

[23] *Darrell Andrews Trucking*, 296 F.3d at 1130-32 (concluding that the agency's adjudicatory opinion in a prior case gave a "crystal clear" interpretation of the regulation).

[24] *Id.* (finding that notice was provided when the agency had previously cited the defendant for regulation violations).

[25] *Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 157 (D.C. Cir. 1986) (Scalia, J.) (holding that notice of a violation given by a non-agency safety inspector did not provide sufficient notice, because it was "not an authoritative interpretation of the regulation"); *see also United States v. Hoechst Celanese Corp.*, 128 F.3d 216, 230 (4th Cir. 1997).

[26] *Gates & Fox Co.*, 790 F.2d at 157 (D.C. Cir. 1986) (Scalia, J.) (holding that notice of a violation given by a non-agency safety inspector did not provide sufficient notice, because it was "not an authoritative interpretation of the regulation"); *see also United States v. Hoechst Celanese Corp.*, 128 F.3d 216, 228, 230 (4th Cir. 1997) (holding fair notice only occurs if the agency's authoritative interpretation is provided to the entity), *cert. denied*, 524 U.S. 952 (1998).

having to parse the statements of agency staff or individual commissioners to determine what the law is.[27]

3. *Did the Agency Inconsistently Interpret the Law or Inconsistently Apply Its Interpretation?*

A fair notice inquiry will look for an agency's conflicting interpretations of the law, *i.e.*, published inconsistent documentation,[28] provided inconsistent advice to entities,[29] or otherwise acted inconsistently.[30] When an agency provided no notice at all, courts would likely exclude this factor.

4. *Imposition of a Serious Penalty*

Finally, the regulation must be sufficiently clear to warn a party of what is expected of it, otherwise, an "agency may not deprive a party of property by imposing civil or criminal liability."[31] The D.C. Circuit seems to view this requirement broadly. According to the court, due

---

[27] In the litigation context, the FTC also has not clearly stated what features of its consent orders are legal requirements. The FTC states that certain data security activities must be *evaluated*, but it does not state that the activities must be implemented. Wyndham FTC Response, *supra* n. 4, at 19 ("Although every situation is different, the consent orders in these matters provide industry, including Wyndham, with notice of different features of data security that must be evaluated in order to maintain a reasonable data security program.").

[28] *See Darrell Andrews Trucking, Inc.*, 296 F.3d at 1130 (stating that the "self-contradictory 'clarifying' utterances" in an agency's formal guidance "could have left [an entity] confused about what was required of it"); *Chrysler Corp.*, 158 F.3d at 1356 (concluding a prior schematic illustrating testing procedures conflicted with the EPA's current interpretation of the testing standard and stating, "[A]n agency is hard pressed to show fair notice when the agency itself has taken action in the past that conflicts with its current interpretation of a regulation."); *Satellite Broad. Co. v. FCC*, 824 F.2d 1, 2 (D.C. Cir. 1987) (finding other sections of the agency's rules "baffling and inconsistent").

[29] *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1332 (D.C. Cir. 1995) (finding that different divisions of the agency disagreed about the meaning of the applicable regulations); *Rollin Envtl. Servs. Inc. v. EPA*, 937 F.2d 649, 653-54 (D.C. Cir. 1991) (finding that agency officials in different regions interpreted the regulation differently and gave conflicting advice to regulated entities); *Gates & Fox*, 790 F.2d at 155 (noting evidence showing that the agency's review board could not agree on the interpretation of the underlying regulation).

[30] *McElroy Elecs.Corp. v. FCC*, 990 F.2d 1351, 1362-63 (D.C. Cir. 1993) (finding that the FCC had "misinterpreted" its own order by telling the defendant it would accept the licensing applications if they were filed, accepting the applications initially, and subsequently rejecting the applications as improperly filed); *Radio Athens, Inc. v. FCC*, 401 F.2d 398, 403 (D.C. Cir. 1968) (noting that five FCC decisions showed that the agency used a different licensing rejection process prior to the process it used to reject the application in the case at hand).

[31] *Gen. Elec.*, 53 F.3d at 1328-29; *see also Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C. Cir. 1986) (Scalia, J.) ("If a violation of a regulation subjects private parties to criminal or civil sanctions, a regulation cannot be construed to mean what an agency intended but did not adequately express[.]" (quoting *Diamond Roofing Co. v. OSHRC*, 528 F.2d 645, 649 (5th Cir. 1976)).

process requires that parties receive fair notice before the government may deprive them of property, such as through the imposition of a fine,[32] the denial of a license application,[33] or by requiring an entity to take costly action, such as a product recall.[34] The D.C. Circuit's "ascertainable certainty" test provides a useful tool to analyze current FTC activities in the area of information security and highlight challenges and complications to the agency's exercise of its § 5 authority.

THE FTC ACT'S PROHIBITION OF "UNFAIR ACTS OR PRACTICES"

In § 5 of the FTC Act, Congress gave broad powers to the FTC to protect consumers from deceptive and unfair trade practices. The FTC has begun using its "unfairness" authority to investigate and punish what it believes are companies' faulty data-security practices. This authority needs to be balanced with the due process rights of entities by memorializing the fair notice doctrine in statute.

THE FTC'S "UNFAIRNESS" AUTHORITY

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[35] An unfair act or practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[36] To be a substantial injury, it must be significant in magnitude and actual (i.e., the harm has occurred or is imminently threatened).[37]

---

[32] *Gen. Elec.*, 53 F.3d at 1328 (concluding that because the agency action resulted in a violation and imposed a fine, fair notice must be reviewed); *Rollins*, 937 F.2d at 653-54 (ruling that a $25,000 fine would be an "imposition of a serious penalty").
[33] *McElroy Elecs.*, 990 F.2d at 1363; *Satellite Broad.*, 824 F.2d at 2; *Radio Athens*, 401 F.2d at 403.
[34] *Chrysler Corp.*, 158 F.3d at 1355 (ruling that a vehicle recall would have required expenditure of significant amounts of money depriving Chrysler of property).
[35] 15 U.S.C. § 45 (a)(1) (2006).
[36] *Id.* § 45 (n).
[37] Letter from the FTC to Hon. Wendell H. Ford and Hon. John C. Danforth, Committee on Commerce, Science and

Consumer injury may involve either causing very severe harm to a small number of people or "a small harm to a large number of people."[38] The two forms of injury that typically qualify under the "unfairness" test are economic harm and harm to health or safety.[39]

The FTC's Use of "Unfairness" Authority

The FTC may use its unfairness authority when the alleged unfair practices and harm to consumers are clear. The FTC has used the law's breadth to regulate a wide range of business practices, from the production of farm equipment[40] to telephone bill processing.[41] However, what constitutes "unfair" data-security practices is far from clear. The amount of data security necessary to make an entity's practice "fair" under § 5 is unknown. Traditionally, the FTC has exercised its unfairness authority when there is obvious and substantial consumer harm, i.e. burn injuries and stolen money. In the vast majority of data-security cases, however, the harm may be more difficult to determine and may not be "substantial." In fact, courts have wrestled with whether the loss of personal information constitutes a cognizable harm to consumers without evidence of actual damages.[42] Actual damages resulting from a particular data-loss incident can be difficult to ascertain.[43] For example, even when a breach compromises credit card numbers,

---

Transportation, U.S. Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in In re Int'l Harvester Co.*, 104 F.T.C. 949, 1070-76 (1984).

[38] *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157 (9th Cir. 2010).

[39] *Int'l Harvester*, 104 F.T.C. at 1086.

[40] *Id.* at 954.

[41] *FTC v. Inc21.com Corp.*, 475 F. App'x 106, 107-08 (9th Cir. 2012).

[42] In the class action context, plaintiffs have faced obstacles in meeting standing requirements when they argue that data breaches result in a cognizable harm, going so far as to claim that paying for identity theft protection services to preempt identity theft is an economic harm caused by the breach. Lower courts have gone both ways on the standing question. *Compare Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011), *Whitaker v. Health Net of California, Inc.*, No. CIV S-11-0910 KJMDAD, 2012 WL 174961, at *2 (E.D. Cal. Jan. 20, 2012), *and Low v. LinkedIn Corp.*, No. 11-CV01468-LHK, 2011 WL 5509848, at *4 (N.D. Cal. Nov. 11, 2011), *with Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010), *Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir. 2008), *and Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007). However, the Supreme Court recently enunciated a strict test for standing when plaintiffs allege a risk of future harm, stating that to confer standing, future harm must be "certainly impending," or at least pose a "substantial risk." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143, 1150 n.5 (2013). Litigants likely will cite *Clapper* in motions to dismiss in class action litigation involving data breaches for the foreseeable future.

[43] The uncertainty of consumer injury in the data-protection context, and the difficulties inherent in identifying it, are discussed in

no harm may result because credit card companies refund consumers for any fraudulent charges made to their account. Given the complexity of data security, the less-than-clear harm, and the fact that third-party criminal activity typically leads to the harm, fair notice is even more essential in the data-security context as compared to other types of alleged unfair practices.

The FTC's Section 5 Enforcement and Penalty Structure

When the FTC identifies an "unfair" practice, it may enforce § 5 against the party using the practice through an administrative process and issue a cease-and-desist order, which commonly results in a consent order.[44] Alternatively, the FTC can file a complaint in court, seeking injunctions and consumer redress against defendants through adjudication and fact finding for alleged violations of § 5.[45]

In the areas of privacy and data security, the FTC has typically followed the administrative process and entered into consent orders with defendants. The full Commission must approve consent orders, and they are subject to notice and public comment before becoming effective.[46]

Any violation of a consent order can result in civil penalties of up to $16,000 per violation,[47] and "[e]ach separate violation . . . [is] a separate offense . . . [and] each day of continuance of such failure or neglect shall be deemed a separate offense."[48] Under this violation calculus, violations and fines can accumulate quickly, and entities face potentially ruinous penalties hanging over their heads for 20 years after entering into a consent order.

---

the briefs of amici curiae in the Wyndham Case.

[44] 15 U.S.C. § 45(b)-(c), (g) (2006).

[45] 15 U.S.C. § 53(a)-(b) (2006).

[46] 16 C.F.R. § 2.34 (2012).

[47] Section 5(1) of the FTC Act, 15 U.S.C. § 45(1) (2006), as modified by Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461 (2006), and Section 1.98(c) of the FTC's Rules of Practice, 16 C.F.R. § 1.98 (c) (2012), authorizes a court to award monetary civil penalties of not more than $16,000 for each such violation of a consent order.

[48] 15 U.S.C. § 45(l).

For example, the FTC filed an action against Google for violating a consent order when Google allegedly used cookies for advertising purposes on Apple Safari users' browsers despite the language in its privacy policy.[49] The result was the FTC's largest fine ever for an order violation: $22.5 million.[50] In its complaint, the FTC alleged that each time Google made a misrepresentation to a user, Google violated the order.[51] Therefore, the FTC appears to have calculated the number of violations based on the number of people who saw the alleged misrepresentations. Considering the number of Google users, the number of people who potentially saw these alleged misrepresentations could be in the millions, and a $16,000 fine for each of a million users would result in a very large civil penalty. Given the potential seriousness of these penalties, the significance of fair notice cannot be understated.

THE FTC USES SECTION 5 OF THE FTC ACT TO INVESTIGATE AN ALLEGED LACK OF PROPER DATA-SECURITY SAFEGUARDS

The FTC Act grants the FTC both specialized rulemaking and enforcement authority under § 5, although the agency's rulemaking authority is limited.[52] The FTC's rulemaking authority, which is commonly referred to as Magnuson-Moss rulemaking,[53] includes additional requirements that are more cumbersome than the more traditional Administrative Proceedings Act (APA) process. For example, the FTC Act requires the FTC to "provide for an informal hearing" in which interested parties are entitled to present oral testimony and potentially cross-

---

[49] Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 1-2, *United States v. Google Inc.*, No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012).
[50] *Id.* at 2.
[51] *Id.* at 7.
[52] 15 U.S.C. § 57a (a)(1)(B) ("[T]he Commission may prescribe . . . rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce . . . .").
[53] *See* Lydia B. Parnes & Carol J. Jennings, Through the Looking Glass: A Perspective on Regulatory Reform at the Federal Trade Commission, 49 ADMIN. L. REV. 989, 995 (1997).

examine witnesses.[54] Due to this potentially inefficient and time consuming process, the FTC has not used its rulemaking authority to issue rules related to data security.[55]

As with formal rulemaking, the FTC has also declined to clarify "fair" data security through formal adjudication. The FTC argues that its consent orders provide fair notice.[56] According to the FTC, it has brought more than 40 data-security enforcement actions since 2000.[57] At least seventeen of those actions alleged unfair practices.[58] However, none of the cases resulted in formal adjudications by the FTC or the courts.[59] Instead, each resulted in a settlement agreement with the respective defendants. The FTC publishes information about its enforcement activity, including the details of the complaints and consent orders,[60] in what some proponents of this approach increasingly refer to as an emerging "common law" of privacy.[61]

The FTC's settlement and consent decree-focused approach to date security consumer protection arguably creates some likelihood of potential actual notice of the agency's interpretation of § 5. The FTC's data-security-related complaints frequently use terms like "reasonable," "appropriate," "adequate," or "proper" to describe the security safeguards that the

---

[54] 15 U.S.C. § 57a(b), (c); *see also* Brief of Amici Curiae Chamber of Commerce of the United States of America, Retail Litigation Center, American Hotel & Lodging Association, and National Federal of Independent Business in Support of Defendants at 21, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-SCM (D. N.J. May 3, 2013) [hereinafter Chamber of Commerce Brief] (noting that "[b]y Congressional Design, [the agency's] rulemaking authority is more burdensome on the FTC than rulemaking authority normally provided to administrative agencies under the APA; among other restrictions, for example, the statute permits interested parties to cross-examine witnesses").

[55] Prepared Statement of the Federal Trade Commission on Data Security: Hearing Before the Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy and Commerce, 112th Cong. 11 (2011) (statement of Edith Ramirez, Comm'r, Federal Trade Commission) ("[E]ffective consumer protection requires that the Commission be able to promulgate rules in a more timely and efficient manner.").

[56] Wyndham FTC Response, *supra* n. 4, at 19.

[57] *Id.* at 13.

[58] *See also* Tech Freedom Brief at 4.

[59] In August 2013, the FTC filed a complaint against LabMD following an alleged data breach. The case was not resolved at the time of this writing. Press Release, Fed. Trade Comm'n, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), available at *http://www.ftc.gov/opa/2013/08/labmd.shtm.*

[60] *Id.*

[61] *See, e.g.*, Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the 12th Annual Loyola University Chicago School of Law Antitrust Colloquium: Privacy, Consumer Protection, and Competition 1 (Apr. 27, 2012), available at *http://www.ftc.gov/speeches/brill/120427loyolasymposium.pdf; see generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy* (Aug. 15, 2013), available at: *http://ssrn.com/abstract=2312913* (last visited Aug. 30, 2013) (contending that the "FTC's privacy jurisprudence is the functional equivalent to a body of common law," and examining it as such).

agency maintains are required under § 5.[62] These complaints, which form the basis of the underlying consent orders, alleged that § 5 was violated due to some combination of failing to: have an information security policy; implement system monitoring; fix known vulnerabilities; maintain firewalls and updated antivirus software; use encryption; implement intrusion detection and prevention solutions; store information only as long as necessary; and prepare for known or reasonably foreseeable attacks.[63] However, because the FTC cryptically states that the failures "taken together" violate § 5 and each complaint lists different data-security practices, these complaints do not provide an effective "data-security blueprint." The FTC's standard mode of operation is to issue non-authoritative suggested guidelines and deal with unfairness actions through settlement. Neither of these practices provide entities with reliable guidance useful in avoiding unfairness actions. Michael D. Scott, a "pioneer" in the field of high-technology law and public policy and graduate of MIT and UCLA School of Law, has criticized the FTC noting that "[t]he complaints and consent orders entered into in these cases provide limited guidance as to what a company should do (or not do) to avoid being the target of an unfairness action by the FTC if it experiences a security breach."[64]

The FTC's consent orders in data-security cases also require some specific data-security practices of those companies whose practices are now supervised directly by the agency,[65] such

---

[62] In its response to Wyndham's motion to dismiss, the FTC reiterated, "unreasonable data security practices are unfair." *See* Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 17, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-CV-01887-ES-SCM (D. N.J June 17, 2013). Some commentators may suggest that there is no security standard because good security varies based on too many factors. This article agrees with that conclusion, but the FTC does not. The FTC seems to be using a security standard when it chooses whether to file complaints against entities for their "unreasonable" security practices. The FTC has issued "guidance" that looks like a standard, but the agency has not communicated that it is the law. Communicating the legal standard to entities will help entities understand what "reasonable" security looks like before they receive the FTC complaint.

[63] Complaint at 2-5, *In re* ACRAnet, Inc., No. C-4331 (Aug. 17, 2011); Complaint at 2-3, *In re* Ceridian Corp, No. C-4325 (June 8, 2011); Complaint at 2-3, *In re* BJ's Wholesale Club, Inc., No. C-4148 (Sept. 20, 2005).

[64] Michael D. Scott, *FTC, the Unfairness Doctrine, and Data Security Breach Litigation*, 60 ADMIN. L. REV. 183 (2008).

[65] *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. 9-11 nn.20-25 (2010) (testimony of Jon Leibowitz, Chairman, Federal Trade Commission) ("The Commission's robust enforcement actions have sent a strong signal to industry about the importance of data security, while providing guidance about how to accomplish this goal.").

as a requirement that the company implement a "comprehensive information security program."[66] The imposed program typically includes: (1) designating employees responsible for data security; (2) implementing reasonable safeguards to protect against identified security risks, including prevention, detection, and response to intrusions; (3) implementing privacy controls appropriate for the business, data use, and sensitivity of the information; (4) and performing regular testing, monitoring, and adjusting of privacy controls. These data-security practices also may give entities some notice of what the FTC believes § 5 requires but whether they are authoritative interpretive documents, given their negotiated, non-precedential nature, lack of judicial review, and agency statement of their non-binding nature, remains an open question.

THE FTC'S PUBLIC STATEMENTS

Even though the FTC has not exercised its specialized hybrid-rulemaking authority to issue any formal data-security rules or regulations, the FTC argues that it "has been investigating, testifying about, and providing public guidance on companies' data-security obligations under the FTC Act for more than a decade"[67] and that companies have sufficient notice "from both government and industry sources," suggesting that companies can follow the NIST, PCI-DSS, or ISO standards.[68] The FTC also argues that its business guidance provides fair notice.[69]

In 2011, the FTC issued *Protecting Personal Information: A Guide for Business*, which lists 36 detailed recommendations related to network security, password management, laptop

---

[66] *E.g.*, Decision and Order at 6-7, *In re* UPromise, Inc., No. C-4351 (Mar. 27, 2012); Decision and Order at 3, *In re* Ceridian Corp., No. C-4325 (June 8, 2011); Decision and Order at 3-4, *In re* Twitter, Inc., No. C-4316 (Mar. 2, 2011) [hereinafter Twitter Decision & Order], available at *http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf.*
[67] *See* Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 7, *FTC v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012).
[68] Wyndham FTC Response, *supra* n. 4, at 17-18.
[69] *Id.* at 18-19.

security, firewall usage, wireless and remote access, and detection of data breaches.[70] Many of the recommendations listed in this publication also appear in the FTC's complaints. The document also explains that "[s]tatutes like . . . the Federal Trade Commission Act may require you to provide reasonable security for sensitive information"[71] although the statute neither refers to "security" nor defines "sensitive information."[72]

The FTC has also been a leader amongst various agencies in using the Internet and social media to disseminate information about the law and best practices. For example, an FTC Web site posting by an FTC attorney states, "[T]he FTC has tried to develop a single basic standard for data security that strikes the balance between providing concrete guidance, and allowing flexibility for different businesses' needs. The standard is straightforward: Companies must maintain reasonable procedures to protect sensitive information. Whether a company's security practices are reasonable will depend on (1) the nature and size of the company; (2) the types of information the company has; (3) the security tools available to the company based on the company's resources; and (4) the risks the company is likely to face."[73] The crux of the constitutional question is when are these settlements, tweets, speeches and blog posts authoritative for interpretive purposes? And, assuming they can be, do they create "ascertainable certainty" the constitutional requires before penalizing a party?

---

[70] FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS, (November, 2011), available at *http://www.business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf.*

[71] *Id.* at 5.

[72] In fact, the troubling constitutional implications of having the government regulate how and what people can say about someone to protect privacy continue to present recurring problems. *See, e.g.*, *Bartnicki v. Vopper*, 532 U.S. 514, 534-35 (2001) (holding that the protections of the First Amendment to disclose information about a public issue trumps the protections against illegally intercepted communications under the Electronic Communications Privacy Act); *see generally* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1050-51 (2000). It is unclear whether the FTC considered these and other potential complications while creating federal "privacy" rights through its actions.

[73] Burke Kappler, *Protecting Personal Information - Know Why*, BUREAU OF CONSUMER PROT. BUS. CTR. (Oct. 2007), available at *http:// business.ftc.gov/documents/art08-protecting-personal-information-know-why.*

APPLYING THE FAIR NOTICE DOCTRINE TO THE FTC'S INTERPRETATION OF SECTION 5

The D.C. Circuit's "ascertainable certainty" fair notice test is a helpful way to examine the FTC's data security enforcement activities to see if what data protection may be *required as a matter of law*. In its fair notice analysis, the D.C. Circuit reviews whether: (1) the plain text of the law is silent or unclear, and the entity's interpretation is plausible; (2) the agency has published clarification of its interpretation or performed other actions providing notice; (3) the agency has made conflicting interpretations; and (4) the entity faces a serious penalty. As described more fully below, in a nutshell, the statutory text is silent, the agency's interpretations are often seemingly unknown or unknowable in the eyes of those prosecuted, the agency maintains it has clarified its interpretations and otherwise provided fair notice and, as a result of these interpretations serious penalties are faced by those prosecuted.

SECTION 5 IS SILENT ON DATA SECURITY

The text of § 5 prohibits "unfair or deceptive acts or practices in or affecting commerce."[74] But the practical difficulties confronting the agency and those subject to its regulation are readily apparent when one refers to the enabling text of the statute itself. The FTC Act prohibits "unfair or deceptive acts or practices,"[75] and leaves the agency with broad authority and discretion to regulate practices that "cause[ ] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[76] Congress intentionally used broad

---

[74] 15 U.S.C. § 45 (a)(1) (2006).
[75] *Id.*
[76] *Id.* § 45(n).

language so the FTC could address unanticipated practices in a changing economy.[77] The language of the statute itself is plain and does not reference any kind of data security or applicable standards for computer software and hardware systems.

THE FTC PUBLICATIONS ARE ADVISORY AND UNCLEAR

When the statutory language does not provide clarity on legally required data-security safeguards, agency statements or activities take on added significance. In particular, a reviewing court should not confine its inquiry to a search for some document listing information that it could label "actual notice," because in most cases evidence will suggest that *some* notice existed. Rather, a reviewing court should focus on whether the provision of notice through methods, such as recommendations and consent orders, constitutes *fair* notice and satisfies due process. Under this analysis, the FTC's recent and historic notice methods in this area remain problematic under the fair notice doctrine, because they do not clearly distinguish the law from best practices or explain why legal requirements may apply in some cases and not others.[78]

The D.C. Circuit conducts a broad inquiry for sources of notice. Previously, it has reviewed regulatory guidance and notices of proposed rulemaking published in the Federal Register,[79] adjudicatory opinions,[80] and agency policy statements.[81] These methods of information dissemination represent statements by the agency about how it intends to interpret the laws it is obliged to enforce. These publications are also sources that organizations may be

---

[77] *See FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1194 (10th Cir. 2009) ("[T]he FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws.").
[78] The FTC argues in Wyndham that industry provides notice of reasonable security standards. Wyndham FTC Response, *supra* n. 4, at 17-18. The legal standard for fair notice reviews what *the agency* states is the law, not what an industry body suggests are best practices.
[79] *Darrell Andrews Trucking, Inc. v. FMCSA*, 296 F.3d 1120, 1130-32 (D.C. Cir. 2002); *United States v. Chrysler Corp.*, 158 F.3d 1350, 1356 (D.C. Cir. 1998).
[80] *Darrell Andrews Trucking*, 296 F.3d at 1130-32.
[81] *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1333 (D.C. Cir. 1995).

expected to review. Conversely, providing information through settlements with individual parties and recommendations posted on an agency website do not seem to rise to the same level of importance, and organizational awareness of these information sources is likely limited.[82]

The FTC Has Not Published Notice in the Federal Register or a Policy Statement

The FTC has not issued any guidance or notices in the Federal Register to explain what it views as adequate data security under § 5. In addition to not using the Federal Register or formal adjudication, the FTC has not published policy statements. As a practical matter, the agency has not yet taken the opportunity to use all of the tools it has to address a serious problem facing industry, who increasingly find themselves feeling twice-victimized.

The FTC Has Used Only Informal Adjudicatory Processes

Agency adjudications are formal actions by an agency, and entities regulated by that agency closely scrutinize them.[83] These adjudications may provide precedential value, and entities are aware that adjudications are policymaking tools for agencies. Therefore, agencies may expect entities to be aware of relevant agency adjudications.

The FTC has not issued any adjudicatory opinions expressing its view on what data-security practices § 5 requires. Instead, as sources of notice, the agency points to the collection of published complaints and the attendant consent orders describing one entity's particular data-security practices that the FTC has deemed inadequate.[84] Courts might consider both sources as

---

[82] More practically, courts have not addressed the question of what types of agency activity should be deemed authoritative for purposes of fairness analysis in ways similar to the analysis of agency deference in *Chevron* or *Mead*.

[83] *See* Steven P. Croley, *Theories of Regulation: Incorporating the Administrative Process*, 98 COLUM. L. REV. 1, 114 (1998) (noting that agency adjudications "sometimes have far-reaching, prospective effects on entire industries," and "often apply prospectively to similarly situated parties not part of the immediate adjudication process").

[84] A collection of complaints and consent orders can be found on the FTC's website. *Legal Resources*, BUREAU OF CONSUMER PROT., *http://business.ftc.gov/legal-resources/29/35* (last visited Aug. 3, 2013). At least one commentator has observed that entities, and their attorneys, scrutinize the FTC's complaints and consent orders as though they were formal

guidance from the agency as a whole under the "ascertainable certainty" test.

Complaints and consent orders are not part of a formal adjudicatory process and do not contain reasoned analysis of the FTC's interpretation of the law.[85] Rather, the complaints list what the FTC believes to be faulty data-security practices in one particular case. The circumstances of each case differ, and, unlike formal adjudications, the FTC has not articulated why data-security practices in one case may violate § 5 while those same practices may not violate § 5 in another context. Moreover, the consent orders are settlement agreements among the parties and have no legal bearing, precedential or otherwise, on third parties.[86] For these reasons, there is little reason for a court to accept such statements as "authoritative" for purposes of evaluating whether they provide constitutionally required fair notice. If regulated entities cannot know with certainty that the complaints and consent orders are the law as applied to them, then the complaints and consent orders may not be sufficiently authoritative to provide fair notice.

An agency can expect an entity that it regulates to comply with policy made through formal adjudication. However, requiring entities to review allegations contained in unfiled complaints with attendant settlement orders begs the question as to whether such actions are suitably authoritative to address fundamental fairness concerns.[87]

Fair Notice Analysis of the FTC's Best Practices Guide

Sadly, for whatever reason, the agency itself has done less than it could to help clarify

---

adjudications. Solove & Hartzog, *supra* n.61, at 25 (discussing that privacy attorneys view FTC settlements like cases interpreting statutes). However, even after careful scrutiny, privacy attorneys cannot definitively advise their clients on what they must do versus what they should do.

[85] *See* TechFreedom Brief at 8 ("Settlements (and testimony summarizing them) do not in any way constrain the FTC's subsequent enforcement decisions . . . [and] unlike published guidelines, they do not purport to lay out general enforcement principles and are not recognized as doing so by courts and the business community.").

[86] *United States v. ITT Cont'l Baking Co.*, 420 U.S. 223, 238 (1975) ("[A] consent decree or order is to be construed for enforcement purposes basically as a contract . . . ."); *United States v. Armour & Co.*, 402 U.S. 673, 681–82 (1971) ("Consent decrees are entered into by parties to a case after careful negotiation has produced agreement on their precise terms.").

[87] *See* Solove & Hartzog, *supra* n. 61, at 24-27 (arguing that the complaints and settlements are in many ways "the functional equivalent of common law").

which of its statements should have the force of law or otherwise provide guidance on the underlying legal requirements for data security. For example, the FTC describes its data security guide, *Protecting Personal Information: A Guide for Business*, as: "Practical tips for business on creating and implementing a plan for safeguarding personal information."[88] The guide suggests to "[u]se the checklists on the following pages to see how your company's practices measure up—and where changes are necessary."[89] The guide does not state that the items in the checklists are required by law or that an entity's compliance with the checklists will ensure that its data security is not an unfair practice. The guide further provides little instruction on when a particular recommendation is a legal requirement or otherwise is or would be a best practice.

Courts, including the D.C. Circuit, have not yet reviewed generally whether an agency's best practices guide provides fair notice of unlawful conduct. If a reviewing court finds that a best practices guide is "authoritative," the court likely would consider the FTC's best practices guide in its analysis.[90] However, there will be a question of the amount of weight a court will give such a guide since it is only a set of recommendations.[91]

Courts place agency action on a spectrum to determine how much deference to afford an agency interpretation of the laws that it enforces. On one end of the spectrum formal rulemaking and adjudication and some informal actions are afforded *Chevron* deference.[92] On the other end of the spectrum are interpretations made by agencies to which Congress has not given sufficient authority. Courts grant those interpretations no deference.[93] To determine whether *Chevron* deference is appropriate for interpretations made outside the context of formal rulemaking or

---

[88] FED. TRADE COMM'N, *supra* n. 70.
[89] FED. TRADE COMM'N, *supra* n. 70.
[90] The D.C. Circuit reviews "public statements issued by the agency." *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995).
[91] Distinguishing between what is required and what is advisory in these guides can be practically impossible without *authoritative* distinctions between the two, an issue frequently discussed among practitioners and agency staff and management.
[92] *Mead Corp.*, 533 U.S. at 229-30.
[93] *See id.* at 231.

adjudications, courts consider whether: (1) Congress intended the agency to interpret the statute with the force of law; (2) the agency action binds only individual parties to a ruling or also applies to third parties; and (3) the interpretation is made by the agency as a whole or by agency staff on an ad hoc basis.[94] The Supreme Court in *United States v. Mead* noted explicitly that interpretations contained in policy statements, agency manuals, enforcement guidelines, and opinion letters do not deserve *Chevron* deference because they lack the force of law.[95]

The FTC Data-Security Best Practices Guide is simply a list of recommendations; it is not the result of formal rulemaking or adjudication and does not bind any parties. It is more similar to the policy statements, agency manuals, enforcement guidelines, and opinion letters that courts have held do not deserve *Chevron* deference. For an interpretation to provide fair notice, it must come from a position of authority.[96] Similarly, staff attorney's Internet postings discussing data security do not represent the entire agency and are not authoritative. Accordingly, a court would probably not appropriately consider the FTC staff attorneys' Internet postings at all in its fair notice analysis. Doctrinally, *Mead* laid important groundwork regarding why much of what the FTC has been saying – especially given its chosen means – raises serious constitutional question of fair notice.

Concerns Stemming from the Lack of Concrete and Authoritative Notice

Consent orders,[97] the FTC's interpretive guidance to entities, consist of little more than published reports and its reliance on consent orders. In particular, the agency has not used its formal rulemaking authority and has not had any formal adjudication through which to

---

[94] *See id.* at 231-34.
[95] *Id.* at 234; *Christensen*, 529 U.S. at 587.
[96] *See Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 157 (D.C. Cir. 1986) (Scalia, J.).
[97] Thirty-six data-security cases were brought under the FTC Act. Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 7, *FTC v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012).

communicate its interpretations. Thus, entities have very little guidance. They have: (1) lists of fairly detailed data-security practices published in single-party complaints; (2) consent orders with vague descriptions of comprehensive information security programs; and (3) published guidance in which the FTC *encourages rather than requires* entities to implement data-security safeguards. With such scant and non-authoritative guidance, the central due process question remains whether such information provides "fair" notice adequate to address constitutional concerns. To be sure, the FTC's published complaints, consent orders, and the aforementioned data-security guide identify many of the same data-security requirements it alleges investigation targets do not adequately maintain. Nevertheless, *some* notice is not *fair* notice—which is a practical constitutional question befuddling many individuals and begging the question: Does reasonable information security require an FTC and administrative law specialist to figure out what the law requires?

Due process requires examining the nature and quality of the notice to ensure entities have a clear description of required behavior from an authoritative source (i.e., fair notice)—which settlements with third parties and agency recommendations do not provide. Moreover, a *post hoc* review of whether sufficient authoritative notice existed *at the time* of the alleged violations is difficult considering an assessment of current requirements is impossible.

Section 5 Violation May Result in Serious Penalty

Under § 5, the FTC cannot directly impose or request a monetary penalty. Congress provided the FTC with the sole remedy to issue an order requiring an entity to cease and desist certain conduct, in part, to avoid potential due process concerns.[98] If a party violates a cease-and-

---

[98] Michael J. Pelgro, Note, The Authority of the Federal Trade Commission to Order Corrective Advertising, 19 B.C. L. REV. 899, 907 (1978).

desist order, a court can order a civil penalty, the rescission of contracts, restitution, refunds, and disgorgement.[99] Alternatively, the FTC can request that a court issue an injunction prohibiting certain behavior.[100] Few would seem to argue that a violation of § 5 could not result in a substantial loss of property implicating the fair notice doctrine.

Given the relative paucity of authoritative agency interpretation, whether existing FTC activities have provided "fair notice" remains an open question. Section 5 of the FTC Act gives the FTC broad authority to combat "unfair trade practices." The statutory language does not provide notice of required data-security safeguards. The FTC has chosen not to issue regulations to explain what data-security practices are "unfair." While the agency's informal communications may provide some notice about the FTC's position, whether courts should deem these communications as sufficiently authoritative to provide fair notice is questionable. Perhaps more importantly, many businesses struggle with understanding what's required of them and are often stunned after a security incident to learn that the party mostly likely to be prosecuted is in fact the organization that held the underlying information—not the perpetrators.

CHALLENGES OF THE FTC'S APPROACH AND MOVING FORWARD

Even if a court concluded that fair notice of required data security practices exists, there seems to be little doubt that underlying legal requirements and the process of determining what is "reasonable" data security could be communicated more effectively. Ironically, an agency that

---

[99] 15 U.S.C. § 45(l) (2006) ("Any person, partnership, or corporation who violates an order of the Commission after it has become final, and while such order is in effect, shall forfeit and pay to the United States a civil penalty of not more than $10,000 for each violation . . . ."); *id.* § 57b(b) ("The court in an action under subsection (a) of this section [an action following a cease a desist order] shall have jurisdiction to grant such relief as the court finds necessary to redress injury to consumers or other persons, partnerships, and corporations resulting from the rule violation or the unfair or deceptive act or practice, as the case may be. Such relief may include, but shall not be limited to, rescission or reformation of contracts, the refund of money or return of property, the payment of damages, and public notification respecting the rule violation or the unfair or deceptive act or practice, as the case may be; except that nothing in this subsection is intended to authorize the imposition of any exemplary or punitive damages.").

[100] *Id.* § 53(b) (allowing the court to issue a temporary restraining order, preliminary injunction, or permanent injunction).

calls on companies to be more transparent about their business practices has not been transparent about its data-security policy, seemingly constrained by the practical difficulties of using investigations and enforcement actions to provide fair notice.

The D.C. Circuit recommended agency rulemaking instead of a series of adjudicative proceedings to explain a regulation because "full and explicit notice is the heart of administrative fairness."[101] The FTC seems to agree that traditional APA rulemaking may be superior to adjudicative proceedings, but it has not yet undertaken to use the modified APA rulemaking authority it already possesses. The FTC has supported federal legislation that would prescribe data-security requirements. The agency recommended that Congress phrase the legislation in general terms, using broad definitions, to allow the implementing agency to promulgate rules or regulations to "provide further guidance to Web sites by defining fair information practices with greater specificity."[102] The FTC stated that regulations could clarify the definition of "adequate security."[103]

FORMAL RULEMAKING MAY PROVIDE FAIR NOTICE BENEFITS

The FTC Has Issued Rules Pursuant to Other Data-Security Related Statutes

While the FTC has not used its current limited rulemaking authority under § 5 to clarify "unfair" data-security practices due to onerous rule-making proceedings, Congress has directed the FTC to promulgate regulations under other laws, such as COPPA and FACTA.[104] As

---

[101] *Radio Athens, Inc. v. FCC*, 401 F.2d 398, 404 (D.C. Cir. 1968) ("[T]he agency could and should have proceeded to accomplish its result by exercising its broad rulemaking powers.").
[102] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 37 (2000) [hereinafter FED. TRADE COMM'N, PRIVACY ONLINE].
[103] *Id.* (internal quotation marks omitted).
[104] *See* 15 U.S.C. § 1681m(e) (FACTA); *id.* § 6502(b)(1) (COPPA).

expected, entities have fully participated in the process.[105] In addition, the FTC altered its proposed rules based on the comments it received.[106] The process and resulting rulemaking have proven far more likely to yield "ascertainable certainty" of the agency's interpretation.

While the final rules the FTC implemented may result in inflexible requirements rather than adaptable principles, the quality of the rules promulgated by the FTC in these instances is beside the point for addressing fair notice concerns.[107] All parties received an opportunity to participate in a public and deliberative process and potentially affect the outcome. The rule-making process also leads to rule refinement outside the enforcement context, which may allow the parties to more objectively view and craft the rules. As it currently stands, recent agency data-security investigations reflect private non-public, refinement of statutory interpretations lacking transparency and clarity. This process runs the practical risk of creating a costly and vexatious guessing game for businesses constrained by a lack of consensus and clarity. The FTC clearly does not intend this consequence. Those subject to FTC data security requirements lack the benefit of any authoritative policy statements on these issues.

Fair Notice Benefits of Rulemaking

There are specific fair notice advantages to rulemaking over the prosecution and settlement approach used by the agency.[108] Rulemaking can provide regulated entities with clear

---

[105] *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3972-73 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312); Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718, 63,718 (Nov. 9, 2007) (codified at 16 C.F.R. pt. 681).

[106] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,889 (Nov. 3, 1999) (codified at 16 C.F.R. pt. 312); Identity Theft Red Flags, 72 Fed. Reg. at 63,719.

[107] Rulemaking is not a panacea. Inflexible rules in a fast-changing environment are problematic. However, the FTC can and should provide clear notice on what the law is. Rulemaking is one method to improve such notice. Rules are not inherently bad, and a principles-based data-security legal framework (rather than a detailed data-security standard) would be one workable solution. The FTC has already articulated 36 detailed recommendations in its guidance. FED. TRADE COMM'N, *supra* n. 70. The FTC has also pointed to the NIST and ISO standards for guidance. Wyndham FTC Response, *supra* n. 4, at 18. The agency holds companies accountable to some or all of these recommendations in some fashion. *Id.* at 17-19.

[108] *See* TechFreedom Brief at 9-10 (noting the ways in which rulemaking is preferable to case-by-case adjudication as a method

guidance, incorporate the thinking of additional stakeholders, prevent cynical speculation regarding agency decision-making, and lessen enforcement and compliance costs.[109] Further, improved notice of a clear rule would likely result in greater compliance.[110] The FTC has not used its existing § 5 rulemaking authority to clarify "unfair" data-security practices because of its alleged impracticality.[111] The FTC does not believe it would "be possible to set forth the type of particularized guidelines" to describe proper data-security safeguards.[112] It has stated that "[d]ata security industry standards are continually changing in response to evolving threats and new vulnerabilities and, as such, are 'so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule.'"[113] The FTC has also stated that "industries and businesses have a variety of network structures that store or transfer different types of data, and reasonable network security will reflect the likelihood that such information will be targeted and, if so, the likely method of attack."[114]

The FTC's statements are mystifying for two reasons. First, if the FTC does not believe that it can properly define "reasonable," fair notice of the reasonableness standard seems unlikely?[115] Second, the FTC seems to have taken the stance that, because technology changes

---

of developing agency-enforced law).

[109] Colin S. Diver, The Optimal Precision of Administrative Rules, 93 YALE L.J. 65, 73, 74 (1983); Brice McAdoo Clagett, Informal Action—Adjudication—Rule Making: Some Recent Developments in Federal Administrative Law, 1971 DUKE L.J. 51, 54-57, 83-84; Bunn et al., No Regulation Without Representation: Would Judicial Enforcement of a Stricter Nondelegation Doctrine Limit Administrative Lawmaking?, 1983 WIS. L. REV. 341, 343-44 (1983).

[110] *See* Diver, *supra* n. 109, at 72, 75.

[111] *Prepared Statement of the Federal Trade Commission on Data Security*, *supra* n. 55, at 11 ("[E]ffective consumer protection requires that the Commission be able to promulgate rules in a more timely and efficient manner.").

[112] Wyndham FTC Response, *supra* n. 4, at 20. At the same time, the White House and Department of Commerce have seemingly articulated an alternative view on prospects for standards development - at least for privacy. "Companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups" have been called together to develop voluntary, enforceable privacy codes of conduct. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 7 (2012) [hereinafter WHITE HOUSE PRIVACY BILL OF RIGHTS], available at *http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf.*

[113] *Id.* (quoting *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947)).

[114] *Id.*

[115] *See* Chamber of Commerce Brief at 12 (noting that "it is *precisely because* the appropriate standards are difficult to ascertain that businesses cannot be held to a nebulous notion of 'reasonableness,' all without any formal guidance before they find

frequently, drafting regulations would be fruitless. However, drafting flexible, principles-based regulations would provide guidance to entities and would still apply as technology changes. The concept of drafting laws in an ever-changing world is nothing new. Moreover, the complaints that the FTC filed a decade ago look similar to the complaints that the agency is filing today.[116] Therefore, the FTC's own actions seemingly contradict that regulations would be impractical or out of date upon publication.

FORMAL ADJUDICATION MAY PROVIDE FAIR NOTICE BENEFITS

A formal adjudicatory process can help provide notice to entities in two ways. When the FTC seeks a formal adjudication, the FTC must report its findings of fact. These findings of fact would clearly and officially communicate, which data-security practices violate the FTC's interpretation of § 5. This mode of operation is superior to the current complaint and settlement process regarding confusion about legal requirements because it puts the FTC on record and may create greater predictability for entities subject to enforcement. To be effective, the agency would need to articulate its interpretation and rationale which the current investigation-complaint-settlement routine does not. Moreover, the FTC or court can publish an opinion, which will further enunciate and clarify the FTC's interpretation. Judicial review also may provide authority supporting the interpretation.

Like rulemaking, this method of clarifying the FTC's interpretation can provide additional benefits, such as improving legal compliance and preventing entities from wasting

---

themselves in violation of the law.").

[116] *Compare* Complaint for Permanent Injunctive and Other Equitable Relief, *FTC v. Wash. Data Res., Inc.*, No. 8:09-cv-02309-SDM-TBM (M.D. Fla. Nov. 10, 2009), *with* Complaint for Permanent Injunction and Other Equitable Relief, *FTC v. SlimAmerica, Inc.*, No. 0:97-cv-06072-DLG (S.D. Fla. Jan. 24, 1997).

resources by attempting to comply with unclear requirements.[117] Nevertheless, adjudication may remain less desirable than rulemaking because regulation by adjudication means that nonparties may not be able to protect their rights.[118] In addition, when regulating by adjudication, the public cannot directly monitor an agency.[119]

ADVISORY OPINIONS, POLICY STATEMENTS, AND OTHER COMMUNICATIONS

Policies made through formal rulemaking and adjudications are more definitively authoritative and can provide entities with clear notice. Advisory opinions, policy statements, analysis appended to proposed consent orders, and other similar communications are less formal and authoritative, but possibly more effective than the current complaint and settlement process and best practice recommendations, as they can communicate agency reasoning and principles.

CONCLUSION

No formal rulemakings or adjudications related to data security have occurred to date, and the FTC appears to regulate data security primarily through complaints and consent orders. This method creates ambiguity because complaints and consent orders are inconsistent or lack additional helpful information. It also is unclear whether nonparties to the investigation should attempt to follow the complaint, the consent order, neither, or both, or whether implementing some or all of the measures would result in "fair" data security. The FTC's position that "security standards can be enforced in an industry-specific, case-by-case manner"[120] provides little guidance. This inherent ambiguity poses dangerous and unnecessary compliance risks for

---

[117] *See* Diver, *supra* n. 109, at 72, 103.
[118] *See* Clagett, *supra* n. 109, at 83.
[119] *See* Bunn, *supra* n. 109, at 343; Clagett, *supra* n. 109, at 56-57 (citing *Holmes v. N.Y.C. Hous. Auth.*, 398 F.2d 262 (2d Cir. 1968); *Hornsby v. Allen*, 326 F.2d 605 (5th Cir. 1964)).
[120] Wyndham FTC Response, *supra* n. 4, at 22.

regulated entities due to the potentially serious penalties that may result from non-compliance.

The FTC's existing enforcement and guidance practices also pose serious constitutional concerns of providing fair notice. Given the current environment of aggressive enforcement against the victims of third-party criminal hacking who operate with no clear guidance what data security actions they should take to avoid allegations of unfair and deceptive acts and practices, improved authoritative interpretations of § 5 are crucial to improve compliance and provide entities with sufficient information to perform proper risk management.

The FTC has several alternative methods for providing more useful and authoritative guidance to entities, but simply stating a vague standard will not improve the situation if it does nothing to clarify the underlying uncertainty or to resolve the problem of fair notice. A "reasonableness" test absent additional, flexible principles-based authoritative guidelines or significant additional court-resolved litigation will remain problematic. As FTC guidance states, "[t]here's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers."[121] In other words, data-security standards may differ as a function of the sensitivity of the data collected, the amount of data collected, and how the data is collected, used, and disclosed to third parties. Using the standards of "reasonable" and "appropriate," without accounting for the nature of the business and the kinds of information that are collected may not ensure that *fair* notice occurs. However, these factors should at least be considered as crucial inputs when determining the data-security safeguards an entity should implement. Nonetheless, such additional standards would still provide no useful guidance without substantial additional stakeholder participation or the reasoned and thorough discussion of the flexible standard in a formal adjudicatory opinion,

---

[121] FED. TRADE COMM'N, *supra* n. 70, at 23.

policy statement, or advisory opinion.

Moreover, even if the FTC employed formal rulemaking or adjudication, the reasonableness test without explanation as currently relied upon by the agency seems less useful in contexts like data security, where the meaning of "reasonable" remains subject to ongoing technological evolution and prevailing data-protection preferences. This is evident now as society continues to debate the balance of strong privacy protections against the societal benefits of the free-flow of information.[122] And notably, the FTC itself does not seem to consistently define what information is "sensitive," potentially deserving greater protection.[123] Thus, there may be no such thing as "reasonable" privacy and data-security practices until a more satisfactory consensus on these issues emerges.

Given the lack of agreement on what "privacy" is, what data should be protected, and what data-security practices should be used to protect that data, any rule based on "reasonableness" should also include explanation. Otherwise, the rule is entirely arbitrary, and "reasonable" security will be whatever the FTC dictates at that point in time. At any given time, an entity would be unable to determine with precision what data-security practices are "reasonable," and whether it could ensure successful compliance with § 5. This situation creates due process challenges and a palpable risk of post-hoc rationalization. For all of these reasons and those laid out above, the agency continues to have a unique opportunity to take up many of

---

[122] WHITE HOUSE PRIVACY BILL OF RIGHTS, *supra* n. 112, at 5-6.

[123] In its recent privacy report, "[t]he Commission defines as sensitive, at a minimum, data about children, financial and health information, Social Security numbers, and certain geolocation data . . . ." FED. TRADE COMM'N, *supra* n. 70, at 47 n. 214. The privacy report also lists passwords as sensitive information. *Id.* at 8, 15, 37 n. 17 4. In other guidance, the FTC includes names that identify customers or employees as sensitive information. FED. TRADE COMM'N, DOES YOUR ORGANIZATION COLLECT AND KEEP SENSITIVE INFORMATION? 1, available at *http://www.business.ftc.gov/sites/default/files/pdf/bus52.pdf.* FED. TRADE COMM'N, *supra* n. 70, at 5. A person's name can hardly be considered sensitive personal information, and the FTC has recently implied that passwords are not sensitive. Press Release, Fed. Trade Comm'n, Tracking Software Company Settles FTC Charges that It Deceived Consumers and Failed to Safeguard Sensitive Data It Collected (Oct. 22, 2012), available at *http://www.ftc.gov/opa/2012/10/compete.shtm.*

the tools it has at its disposal to address the practical problem that businesses face in being unable to determine better what data security measures are required as a matter of law and which practices are simply better or best.

Chairman ISSA. Mr. Hartzog.

STATEMENT OF WOODROW HARTZOG

Mr. HARTZOG. Chairman Issa, Ranking Member Cummings, and members of the committee, thank you very much for inviting me to provide testimony today. My name is Woodrow Hartzog, and I'm an associate professor at Samford University's Cumberland School of Law and affiliate scholar at the Center for Internet and Society at Stanford Law School. I am testifying today in my personal academic capacity, and not on behalf of any entity.

For the past 2 years, my coauthor, Daniel Solove, and I have researched the Federal Trade Commission's regulation of privacy and data security breaches, which I will collectively call data protection. We have analyzed all 170-plus FTC data protection complaints to find trends and understand what the FTC's data protection jurisprudence actually tells us. I would like to make two main points regarding what I've learned about the FTC's regulation in this area.

First, the FTC's regulation of privacy and data security under Section 5 has served a vital role in the U.S. system of data protection. The FTC's involvement has given a heavily self-regulatory system of data protection necessary legitimacy and heft. The FTC also fills significant gaps left by the patchwork of statutes, torts, and contracts that make up the U.S. data protection scheme.

The FTC's regulation of data protection also helps foster consumers' trust in companies. It is very difficult for consumers to determine whether a company has reasonable data security practices or not. The FTC's regulation of data protection helps give consumers confidence that their personal information will be safe and properly used.

The second point that I would like to make is that the overwhelming pattern that is apparent from the FTC's data protection jurisprudence is that the agency has acted judiciously and consistently in outlining the contours of impermissible data protection practices. Section 5 of the Federal Trade Commission Act generally prohibits unfair or deceptive trade practices. This is an intentionally broad grant of authority. Congress explicitly recognized the impossibility of drafting a complete list of unfair, deceptive trade practices. Any such list is destined to be quickly outdated or easily circumvented.

Despite this broad grant of authority, the FTC actually brings relatively few data security complaints, especially compared to the total number of reported data breaches. The Privacy Rights Clearinghouse has reported that since 2005, there have been over 4,300 data breaches made public, with a total of 868 million records breached. Yet the FTC has filed only 55 total data security-related complaints, averaging around 5 complaints a year since 2008. Instead of attempting to resolve all of the data breaches, the FTC typically pursues only what it considers to be the most egregious data security practices.

The FTC has used a reasonableness standard to determine what constitutes an unfair, deceptive data security practice. What constitutes reasonableness is determined virtually entirely by industry standard practices, and is contingent upon the sensitivity and vol-

ume of data, the size and complexity of a company, and the costs of improving security and reducing vulnerabilities. This deference to industry keeps the FTC from creating arbitrary and inconsistent data rules.

The FTC does not pull rules out of thin air. Rather, it looks to the data security field and industry to determine fair and reasonable practices. Virtually all data security regulatory regimes which use a reasonableness approach, of which there are many, not just the FTC, have four central requirements in common: identification of assets and risks; data-minimization procedures; administrative, technical and physical safeguards; and data breach response plans. The details of these requirements are filled in by industry frameworks, accessible resources online, and a vast network of privacy professionals and technologists dedicated to helping companies of all sizes understand their data protection obligations.

Of course there is always room for improvement with any regulatory agency, but diminishing FTC power will probably not ultimately make the climate easier for business. In fact, given the vital importance of data protection in commerce, a reduction in FTC authority would likely result in the passage of more restrictive and possibly conflicting State laws regarding data security, more actions by State attorneys general, more lawsuits from private litigants, and more clashes with the European Union over the legitimacy of U.S. privacy law. In the long run, a weakened FTC would likely result in a more complicated and less industry-friendly regulatory environment.

Data protection is a complex and dynamic area for consumers, companies, and regulators. Section 5 enables the FTC to be adaptive and serve as a stabilizing force for consumers and companies. Thank you very much.

Chairman ISSA. Thank you.

[Prepared statement of Mr. Hartzog follows:]

PREPARED TESTIMONY AND STATEMENT FOR THE RECORD
OF

WOODROW HARTZOG
ASSOCIATE PROFESSOR OF LAW
SAMFORD UNIVERSITY'S CUMBERLAND SCHOOL OF LAW

HEARING ON

"THE FEDERAL TRADE COMMISSION AND ITS SECTION 5 AUTHORITY: PROSECUTOR, JUDGE, AND JURY"

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

July 24, 2014
2154 Rayburn House Office Building
Washington, DC

I. INTRODUCTION

Chairman Issa, Ranking Member Cummings, and Members of the Committee, thank you for inviting me to appear before you and provide testimony. My name is Woodrow Hartzog and I am an associate professor of law at Samford University's Cumberland School of Law and an affiliate scholar at the Center for Internet and Society at Stanford Law School. I write extensively about information privacy law issues and have published well over a dozen law review articles and other scholarly works. Most relevant to this hearing, I, along with my co-author Professor Daniel J. Solove, have spent the last two years researching the Federal Trade Commission's regulation of privacy and data security issues, which I will collectively refer to as "data protection." In a series of articles, we have analyzed all 170+ FTC data protection complaints to find trends and understand the FTC's data protection jurisprudence.[1] My comments today will address what I've learned from this research.

I will focus my remarks on the FTC's work on data security and consumer privacy, and especially the scope of the FTC's authority to regulate data protection under Section 5 of the FTC Act. I will not address the specifics of any particular privacy or data security dispute. These comments are made in my personal, academic capacity. I am not serving as an advocate for any particular organization. My remarks will focus on two points.

First, I will discuss why the FTC's regulation of privacy and data security under Section 5 has served a critical function for the US system of data protection. Far from being an overall burden to industry, the FTC's involvement in data protection has given the heavily self-regulatory system of data protection necessary legitimacy and heft. Diminished FTC data protection authority would threaten the existence the U.S.-E.U. Safe Harbor which governs the international exchange of personal information. No other regulator has the same ability to enforce necessary yet quickly evolving protections like data security.

Second, I will discuss the scope and administration of the FTC's Section 5 authority. I have spent a considerable amount of time analyzing the entire body of FTC activity on data protection. Overall, the overwhelming pattern is that the FTC has acted conservatively, judiciously, and consistently. Given the ever increasing volume of data and accompanying risk of the information age, the role of the FTC in data protection seems both important and a natural consequence of the agency's charge to protect consumers.

---

[1] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014), available at http://ssrn.com/abstract=2312913; Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015), available at http://ssrn.com/abstract=2461096; Daniel J. Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, 13 BNA PRIVACY & SECURITY LAW REPORT 577 (2014), available at http://ssrn.com/abstract=2424998; Woodrow Hartzog & Daniel J. Solove, *The FTC as Data Security Regulator: FTC v. Wyndham and its Implications*, 13 BNA PRIVACY & SECURITY LAW REPORT 621 (2014), http://docs.law.gwu.edu/facweb/dsolove/files/BNA%20FTC%20v%20Wyndham%20FINAL.pdf.

II. SECTION 5 IS THE LYNCHPIN OF U.S. DATA PROTECTION LAW

The most important grant of authority to the FTC in protecting consumers' personal information comes from Section 5 of the Federal Trade Commission Act. Under this statute, "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[2] The FTC first began to regulate data protection online in the 1990s by focusing on promises companies voluntarily made in their privacy policies. When companies later failed to live up to these promises, the FTC claimed that this was a deceptive trade practice.

In this way, the FTC used the predominantly self-regulatory approach to privacy and data security as its foundation to build a foothold in the area of data protection. Over time, the FTC expanded beyond enforcing privacy policies to a broader conception of deception, one that did not rely only on explicit promises made. The FTC also began to exercise its power to police unfair trade practices.

Today, the FTC has evolved into the most important data protection agency in the United States. The FTC plays two critical roles within the U.S. data protection ecosystem. It fills significant gaps left by the patchwork of statutes, torts, and contracts that make up the U.S. data protection scheme. The FTC also stabilizes the volatile and rapidly evolving area of data protection and provides legitimacy for the largely sectoral U.S. approach to data protection.

A. Filling Critical Gaps

In the current U.S. privacy regulatory system, the FTC has grown into the key lynchpin giving coherence to a partly self-regulatory system supported by a loose patchwork of data protection laws at the federal and state level. Unlike many other countries, in the U.S. there are a multitude of different laws regulating different industries rather than just one general law to regulate all collection and use of personal data.

Particular sectoral laws often leave gaps where entire industries lack privacy regulation. For example, there is no federal law that explicitly mandates data security for all online commerce. Without the FTC, some collections and uses of data would be unregulated. Through Section 5, the FTC sets a floor for commercial activity that otherwise cannot be practically regulated by consumers through contract, tort, or reputation.

Concerned about consumer concerns and trust, in the late 1990s online companies began voluntarily making promises about data protection in privacy policies. Initially, the FTC began enforcing these promises made in privacy policies, giving the promises a stronger backbone. The FTC's broad range of coverage spanned countless industries, thus plastering over the large gaps and crevices left in between sectoral laws. The FTC also brought a thin layer of coherence to the whole system, and this coherence has gradually thickened over the years.

[2] 15 U.S.C. § 45(a)(1).

The FTC currently remains a key lynchpin in the U.S. data protection regulatory regime. Self-regulation still plays a big role, with industry serving as the primary generator of best practice norms. Far from being externally imposed, the norms that the FTC has enforced have been developed by industry as well as consumer expectations. Instead of imposing top-down rules all at once, the FTC has integrated itself into a largely self-regulatory approach and gradually developed it into a more robust regulatory system.

B. The Stabilizing Function of the FTC

The FTC also stabilizes and legitimizes the U.S. approach to data protection. For example, the FTC plays a pivotal role in international confidence regarding privacy in the United States. The FTC is an essential component of the Safe Harbor Arrangement, which allows personal data to flow between the United States and European Union.[3] Without the FTC's data protection enforcement authority, the E.U. Safe Harbor agreement and other arrangements that govern the international exchange of personal information would be in jeopardy.

With so many different sources of law and regulation in the United States, the FTC can also play a harmonizing role. The broad scope of Section 5, which allows the FTC to respond to many different kinds of threats to data protection, can obviate the need for new laws. Section 5 ensures fewer gaps and fewer needs of states to protect their citizens in possibly very conflicting and burdensome ways. The FTC's power is broad enough to develop over time a more coherent and comprehensive body of regulatory activity.

III. THE SCOPE AND ADMINISTRATION OF THE FTC'S AUTHORITY UNDER SECTION 5

The FTC's most important tool for protecting the data of consumers is its grant of authority to regulate unfair and deceptive trade practices under Section 5. Congress granted the FTC the authority to interpret the nature of deceptive practices, which the agency summarized in a 1983 policy statement: A deceptive trade practice is a "misrepresentation, omission or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment."[4] Unfair trade practices are defined by statute as a practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[5] This broad

[3] See, e.g., Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7, 26–30 (discussing FTC enforcement authority); Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000) (same); Int'l Trade Admin., U.S. Dep't of Commerce, U.S.-EU Safe Harbor Overview, Export.gov, http://www.export.gov/safeharbor/eu/eg_main_018476.asp_ ("Under the Federal Trade Commission Act, for example, an organization's failure to abide by commitments to implement the Safe Harbor Privacy Principles might be considered deceptive and actionable by the Federal Trade Commission.").

[4] Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983) , reprinted in In re Cliffdale Assocs., Inc., 103 F.T.C. 110 app. at 175–84 (1984) (decision & order).

[5] 15 U.S.C. § 45(n) (2012).

grant of authority was designed precisely to avoid restrictive categories of practices which are unfair or deceptive.[6]

A. The Intentionally Broad Scope of Section 5

Other than the limitations inherent in the conceptualizations above, Congress has been explicit in eschewing hard boundary lines for what constitutes unfair and deceptive trade practices.

The scope of the FTC's deceptiveness jurisdiction has included broken promises of privacy and data security, deceptive actions to induce the disclosure of information, and failure to give sufficient notice of privacy invasive practices. Although the requirement that a deception be material to consumers constrains the scope of FTC enforcement power, misrepresentations can be made in virtually any context, including boilerplate policies, marketing materials, and even the design of websites.

The FTC's unfairness authority is also comprehensive. According to the FTC, "The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[7]

B. A Conservative, Judicious, and Consistent Approach

A review of every FTC complaint related to data protection reveals that the agency has acted in a conservative way. The FTC's data security program began under the direction of then-Chairman Timothy Muris and has continued, without any major course change, under the stewardship of Chairwoman Deborah Majoras, Chairman William Kovacic, Chairman Leibowitz, and now Chairwoman Ramirez.

The FTC actually brings a relatively very small number of data security complaints. Compared to the number of total reported data breaches, the likelihood that a company will be subject to a FTC enforcement action is quite low. The Privacy Rights Clearinghouse has reported that since 2005 there have been over 4300 data breaches made public with a total of over 868 million records breached.[8] Yet the FTC has filed only 55 total data security-related complaints, averaging around five complaints a year since 2008.[9]

---

[6] *See* H.R. Conf. Rep. No. 1142, 63d Cong., 2d Sess., at 19 (1914) (finding that, regarding unfairness, if Congress "were to adopt the method of definition, it would undertake an endless task").

[7] FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). *See* 15 U.S.C. § 45(n). *See also* CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (forthcoming 2015).

[8] PRIVACY RIGHTS CLEARINGHOUSE, *Chronology of Data Breaches: Security Breaches 2005 – Present*, https://www.privacyrights.org/data-breach.

[9] FEDERAL TRADE COMMISSION, *Legal Resources: Privacy and Security*, http://www.business.ftc.gov/legal-resources/29/35.

Instead, the FTC typically pursues only what it considers to be egregious data security practices. Each data security complaint includes a litany of alleged security failures, including failures to identify assess and risk, failures to minimize the storage of data, and failures to implement reasonable administrative, technical, and physical safeguards. The FTC has remained notably consistent as it gradually develops its data security jurisprudence in incremental steps.

C. The Wide Consensus of Reasonableness-based Data Security Requirements

The FTC generally prohibits unreasonable data security practices "in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[10]

What constitutes reasonable data security is determined virtually entirely by industry standard practices. This deference to industry keeps the FTC from promulgating data security rules in an arbitrary and inconsistent way. The FTC does not pull rules out of thin air. Rather, it builds upon the formidable and evolving body of knowledge in the data security field as well as the commonly implemented data security practices of companies to determine when custodians of personal information are engaging in unfair and deceptive data security practices.

A reasonableness standard is already one the most established and proven touchstones for regulating data security. Almost ten states require reasonable data security practices, rather than a specific list of prohibited or mandatory actions.[11] Congress has also explicitly embraced a reasonableness approach to data security. The Fair Credit Reporting Act (FCRA),[12] the Health Insurance Portability and Accountability Act (HIPAA),[13] and the Gramm-Leach-Bliley Act (GLBA)[14] all use reasonableness as a touchstone for determining the adequacy of data security measures.

Unfortunately, it is not possible to provide a "one size fits all" detailed checklist of reasonable data security practices. A determination of reasonable data security is far too dependent upon context. Yet a comparison of data security regulatory regimes that use a reasonableness standard shows that there are four central components of a reasonable approach to data security:

1) Identification of assets and risk
2) Data minimization
3) Administrative, technical and physical safeguards
4) Data breach response plans

---

[10] FEDERAL TRADE COMMISSION, *Commission Statement Marking the FTC's 50th Data Security Settlement* (January 31, 2014) http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
[11] *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015) at fns 80-83, available at http://ssrn.com/abstract=2461096.
[12] 16 C.F.R. § 682.3(a).
[13] 45 C.F.R. §§ 164.308-.314.
[14] 16 C.F.R. §§ 314.3-314.4.

Various frameworks exist to provide further detail for those operating in certain contexts, such as the framework and standards offered by the National Institute of Standards and Technology (NIST)[15] and the Payment Card Industry (PCI) Security Standards Council.[16]

Additionally, ample resources exist for companies looking for guidance on reasonable data security practices, many of which are free and easily accessed online. The Federal Trade Commission actively updates its resources on data security.[17] Scholarly articles, trade publications, and other sources of information are also readily available.[18]

A robust support system exists for companies seeking to provide reasonable data protection for consumers. There is a vast network of privacy professionals dedicated to helping companies understand their obligations under certain privacy regimes like the FTC. Technologists and other consultants can help companies of all sizes. These counselors have a nuanced understanding of data protection and the significance of the FTC complaints and are able to rely on the FTC's guidance as well as industry standards to competently advise their clients.

IV. CONCLUSION

Section 5 of the FTC Act has empowered the Federal Trade Commission to serve a central role in protecting consumer information. Just as importantly, the FTC's data protection jurisprudence helps create and sustain consumer trust in companies that collect and store consumers' personal information. It is very difficult for consumers to determine whether a company collecting their personal information has reasonable data security practices. This opacity decreases the incentive for companies to spend the resources necessary to establish reasonable data protection. The FTC's regulation of data protection under Section 5 allows consumers to transact with companies with greater confidence that their personal information will be safe and properly used.

Of course, as with any agency, there is always room for improvement of FTC enforcement. More detailed complaints and closing letters from investigations that do not result in a complaint are quite helpful to other companies and, to the extent that they are productive and feasible, should be encouraged. But the agency's power should be expanded rather than contracted. Diminishing FTC power will not ultimately make the climate easier for business. In fact, given the vital importance of data protection in commerce, a reduction in FTC authority would likely result in the passage of more

---

[15] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Framework for Improving Critical Infrastructure Cybersecurity*, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[16] PCI SSC Data Security Standards Overview, https://www.pcisecuritystandards.org/security_standards/.

[17] FEDERAL TRADE COMMISSION, *Legal Resources: Privacy and Security*, http://www.business.ftc.gov/legal-resources/8/35.

[18] *See, e.g.* Joel Reidenberg, N. Cameron Russell, Alexander Callen, and Sophia Qasir, *Privacy Enforcement Actions*, CENTER ON LAW AND INFORMATION POLICY (June 2014), http://law.fordham.edu/assets/CLIP/CLIP_Privacy_Case_Report_-_FINAL.pdf; Travis D. Breaux & David Baumer, *Legally "Reasonable" Security Requirements: A 10-year FTC Retrospective*, 30 COMP. & SECURITY 178 (2011), http://www.cs.cmu.edu/~./breaux/publications/tdbreaux-cose10.pdf.

restrictive and conflicting state laws, more actions by state attorneys general, more lawsuits from private litigants, and more clashes with the E.U. concerning the overall strength of U.S. privacy law. In the long run, a weakened FTC would likely result in a more complicated and less industry-friendly regulatory environment.

Data protection is a complex and dynamic area. Section 5 enables the FTC to be adaptive and serve as a stabilizing force for consumers and companies.

Chairman ISSA. I will now recognize myself for a round of questioning.

Mr. Daugherty, there was an allegation by Tiversa that there was a data breach. Have you seen ever any indication, collateral indication, that that breach went to third parties that resulted in any use of the identity information? Any?

Mr. DAUGHERTY. Thank you, Chairman Issa.

As a matter of fact, no, sir, we have not.

Chairman ISSA. Okay. Mr. Roesler, same thing. You put up with years of a lawsuit. Did any of the complainants have any demonstrated information that their identifiable information had actually gone somewhere, or just that there was a vulnerability?

Mr. ROESLER. To my knowledge, there is none.

Chairman ISSA. Now, if there was a breach, meaning it was taken—you had what was it, 184 records that were alleged? Mr. Daugherty, you had thousands?

Mr. DAUGHERTY. Correct. Nine thousand.

Chairman ISSA. I've heard an expression that I'd like to see if you all agree with. If you have thousands of records, whether it is 184 in your case or many, many thousands, if they have actually gone out to third parties somewhere, they've, in other words, mined them, doesn't it defy gravity that none of them have led to any use of that information in either of your cases?

Mr. DAUGHERTY. Yes, Chairman Issa, I would agree with that.

Chairman ISSA. Okay. So I'm not a student of statistics, but I had to take it in college. I certainly agree.

So the allegation that you're facing is that you had a vulnerability, not an actual breach in reality, because a breach would demonstrate some use. What they really said was, Mr. Roesler, you didn't protect your site, you didn't have a good enough lock on your site; is that correct?

Mr. ROESLER. I believe so, yes.

Chairman ISSA. Mr. Daugherty, same thing. Your lock wasn't good enough.

Mr. DAUGHERTY. That's correct, sir.

Chairman ISSA. Now, the American people may not understand cybersecurity at this point, but they understand the padlock on their front door, their garage door opener. And I just want to put it in perspective for a moment.

Ninety percent of the garage door openers made before the year 2000, a product that simply takes the chip and sequentially goes through the combinations, will open every one of those garage doors. Before 2000, the vast majority of garage doors, simply you had to go through anywhere from 250 to a few thousand combinations, and eventually your garage door would open. People haven't gone back and changed their garage doors. Unless you have a Medeco key or a number of other very high-security keys, if you have a typical key, it can be picked by any locksmith.

So are these people leaving a vulnerability? Maybe yes, maybe no. But I want to put it in perspective for both of you.

The allegation, as I understand it from previous testimony before this committee, is effectively one of your employees may have installed a program that was sort of the equivalent of putting a little bit of bubble gum in the door latch so that the door didn't really

lock, and there was a vulnerability. In both cases, as far as I understand, there was no allegation that you instructed the employee to do it, or that you did it, or that it was done with your knowledge. And, Mr. Roesler, I understand in your case you never found the alleged peer-to-peer; is that correct?

Mr. ROESLER. That's correct. And I don't know that the allegations were ever about an employee. Simply that a file that Open Door had created had gotten out.

Chairman ISSA. Right. But a file that was never found except in the hands of Tiversa.

Mr. DAUGHERTY. Same. As a matter of fact, if you look at the FTC's press release announcing the litigation, they never used the word "breach." That's correct, sir.

Chairman ISSA. So we're not talking about a loss of data, we're talking about the vulnerability, the same vulnerability that every time a notebook like this or a computer notebook walks out of a government office with personal information on it, like it did in the case of the famous VA one where somebody simply left their notebook, and a million veterans' identifiable information was there, it's a vulnerability. If it actually occurs, it occurs because of a human failure in most cases, not because of an inherent system failure.

Mr. Daugherty, you were running a dotcom. Did you have professional advice and counsel, and did you buy software to protect against this type of thing?

Mr. DAUGHERTY. We ran a medical laboratory.

Chairman ISSA. But, I mean, you had an online presence.

Mr. DAUGHERTY. We had an online presence.

Chairman ISSA. Mr. Roesler, same thing. From your testimony, you engaged professional outside people to give you security.

Mr. ROESLER. That's correct.

Chairman ISSA. So you used what you would consider and still consider to be maybe not best practices, but the best practices you knew of and could afford, right?

Mr. ROESLER. Yes.

Chairman ISSA. We were told under oath by Mr. Boback twice that, in fact, deceptive software was what they went out looking for and found these breaches. And I just want to close by asking just one question.

Mr. Roesler—and I keep mispronouncing it.

Mr. ROESLER. It's Roesler.

Chairman ISSA. Roesler. Mr. Roesler, in your case you had a kind of a unique thing that I want to make sure you get a chance to explain to us. A company, Tiversa, in Pittsburgh, more or less, contacts you. Coincidentally a plaintiff's law firm in Pittsburgh, Pennsylvania, as I understand it, forms a class-action lawsuit and goes after you, and has the information to contact those very people who they told you you had this breach. So the law firm has the name of all your clients; is that right?

Mr. ROESLER. That's exactly right.

Chairman ISSA. And they didn't get it from you. So in your case you do have a breach. You know that somebody clandestinely got your clients', your AIDS patients' information, gave it to a law firm who then used it—and I ask unanimous consent that the sample—we'll get it here in a second—letter that that law firm sent out to

every one of your patients—this is called Serrano and Associates—and it says right on the bottom, this is a solicitation to provide legal services. And is this a copy for the ranking member? I'll give a copy to the ranking member. You have seen that solicitation?

Mr. ROESLER. Indeed.

Chairman ISSA. So I just want to make sure for the record that both sides understand. Tiversa contacts you and says there's been a vulnerability, offers you to sell you the services for nearly $500 an hour. You turn them down after talking to your professionals, find no vulnerability. But then a law firm has the very information they were talking about, which obviously was gleaned somewhere, and probably off of your servers or your drives. They—then it gets somehow to a law firm, coincidentally in Pittsburgh, who then goes about creating a plaintiff's—a class-action suit, contacts your patients, who in no other way were contacted except by this law firm, and proceeds to sue you for years.

Mr. ROESLER. That is my perspective.

Chairman ISSA. Okay. I now recognize the ranking member.

Mr. CUMMINGS. Mr. Chairman, to indulge us before I ask my questions, I would ask for just 1 minute to clarify a point for the record with unanimous consent with regard to some statements you made in your opening statement. May I?

Chairman ISSA. Go ahead.

Mr. CUMMINGS. Thank you very much.

The chairman made some points in his opening statement about the potential immunity for a witness, and I take this moment because, Mr. Chairman, everybody on both sides of the aisle care tremendously about whistleblowers. There is not one person on this, Republican or Democrat, and our record has shown that.

You said that the Democrats have been unwilling to consider immunity. That's not accurate. We have said consistently and repeatedly that we are willing to consider immunity. We participated in the proffer. We viewed the video, as well as many documents. At this stage the committee has not identified evidence that would substantiate or corroborate the allegations of this witness against other individuals.

The chairman also said that we have sought out negative information about this witness in an effort to discredit him. That's not true. The information came to us from the CEO of Tiversa's attorney about criminal activity. Once we found out about that, we wanted to know more about it. I mean, that's just logical.

Chairman ISSA. I thank the ranking member, and I would say that this is perhaps outside the scope of this hearing. I would also note——

Mr. CUMMINGS. But you just made these allegations against us. It's in the scope of the hearing because you put it in there.

Chairman ISSA. You asked unanimous consent. I granted it. The fact is that my opinion in the opening statement will stand.

I will say for the record, since you just said it, too, the fact is your committee members have refused—even sitting here in the House of Representatives, even inside a building with total security, they have refused to meet with the whistleblower, claiming that based on the allegations of Mr. Boback and his attorney, that they are too afraid to, men and women. So quite frankly, you can

have your opinion—you can have your opinion, Mr. Ranking Member, I will have mine.

Mr. CUMMINGS. Very well. I will continue my 5 minutes then.

Chairman ISSA. I will start your 5 minutes over in a moment.

Mr. CUMMINGS. Okay.

Chairman ISSA. I have invited in my opening statement, and with indulgence of the witnesses, all Members to look at the video proffer, and all members of this committee to have access directly to the whistleblower for purposes of continuing the proffer.

I made it clear in my opening statement—and I will reiterate it because I think the ranking member's point is good—serious allegations about the personal life of the witness have come forward. But, again, as I said in my opening statement, allegations do not go to the direct claims of the whistleblower as to the facts that he said in his proffer had occurred.

So is the whistleblower claiming he did no wrong? Just the opposite. The whistleblower has come forward with a proffer, because, in fact, if he makes that testimony, he will do so at the risk of prosecution. The whistleblower has already taken the Fifth in another venue, and, as a result, qualifies for the question.

Now, in the Lois Lerner case, Mr. Cummings, we had a witness who you kept saying you wanted immunity for, but she only said she was innocent. In this case we have an individual——

Mr. CUMMINGS. There you go again.

Chairman ISSA. This individual, this individual came forward and said wrongdoing occurred. It has led to today's hearing. And I simply, in my opening, asked all Members to take the time to look at the information individually, because I do believe that to get a full understanding and cross-dialogue—because everything that is brought out by our whistleblower is subject to, in fact, credibility check as to the facts brought—but that dialogue will not be possible unless the whistleblower is granted the limited immunity as to exactly what, and only what, he came forward with as allegations against Tiversa, and, as a result, the FTC and perhaps false statements made before this committee.

It is a serious claim, I take it seriously, and I ask all Members to individually look at it. Mr. Cummings, most Members have never seen any of it, and that's why I was making it available today in open hearing to look at it and make their own decisions.

And I thank the gentleman. Please restore his time to 5 minutes.

Mr. CUMMINGS. Thank you, Mr. Chairman.

The chairman also said we had sought out negative information about this witness in an effort to discredit him. That is not true. The witness has engaged in numerous criminal activities that go to credibility, and he failed to disclose to the committee during his proffer, he failed to disclose them. And some of these activities were occurring at the same time that we were speaking with the—that he was speaking with the committee.

Generally, I believe the committee should grant immunity to witnesses who have admitted to engaging in criminal conduct only in rare circumstances when those witnesses provide concrete evidence of criminal activity by others. I appreciate the goal of rewarding whistleblowers who come forward voluntarily to identify waste, fraud, and abuse, and we have a record of that. But I do not believe

that immunity is a proper reward when individuals provide evidence relating only to their own wrongdoing.

Although we remain open—and I say, I want to be clear—although we remain open to considering immunity should additional evidence emerge, we cannot responsibly support immunity at this time.

Now, according to the Republican memo for today's hearing, one of the main topics is, "whether the FTC has the authority to pursue data-security enforcement actions under its current Section 5 authority." So let's ask our witnesses.

Mr. Stegmaier, you have written extensively on this topic. In one article, you wrote, "The agency is the Federal Government's largest consumer protection agency. The Commission routinely investigates publicly reported data-related incidents with the threat of subsequent litigation. Since 2000, the FTC has brought 42 data-security cases."

Mr. Stegmaier, with respect to the hearing question today, I take it from your writings that you agree that the FTC has the authority to bring enforcement actions under Section 5 to protect the data security of consumers; is that right?

Mr. STEGMAIER. Mr. Cummings, thank you. That is actually a really great question, and I appreciate the way that you have presented it.

At the outset, let me just note that I come before the committee today with the understanding that the committee sought my expertise and understanding specifically about fair notice and due process concerns.

Whether or not the agency has jurisdiction is actually, ironically, something that Congress has given the agency incredible deference to determine in and on its own, and it's actually subject to a number of pending lawsuits and litigation.

So the answer to your question, I think, is that the agency absolutely believes that it has such jurisdiction, but that answer to that question hasn't been definitively resolved. And, historically, under caselaw, the agency would receive such deference.

But my focus is more on whether or not people who are going to be subject to that deference, whatever the ultimate outcome may be, have fair notice about what the law requires of them.

Mr. CUMMINGS. Mr. Hartzog, you have also written extensively on the FTC's work on data security, so let me ask your expert opinion. Does the FTC have the authority to bring data-security actions under Section 5?

And one of the things that we should all be concerned about is a chilling effect. And I just wanted you to respond to that.

Mr. HARTZOG. Sure. I think that, yes, the FTC does have the authority under Section 5 to regulate data-security practices. If you look at the plain wording of Section 5, it is intentionally quite broad. There are limitations, so, you know, there are limits as to what constitutes an unfair practice and a deceptive trade practice. But, certainly, you know, given the heft of both the opinion, the recent opinion, in the Wyndham decision and the FTC's practice generally in the way that we interpret statutes, the FTC has the authority to regulate data security.

With respect to chilling effects, I think that the FTC has proceeded in a pretty judicious and conservative manner with respect to the regulation of data security, and so it is not like there has been a dramatic lurch forward. As a matter of fact, they have been inching along through several different Presidential administrations basically along the exact same course with no appreciable difference. And so I think that the body of jurisprudence is actually sound in that regard.

Mr. CUMMINGS. Professor, can you describe why it is important for the FTC to exercise its authority over data-security breaches?

Mr. HARTZOG. Sure. There are several reasons. One is it gives the U.S. system of data protection legitimacy and heft. So many, for example, international agreements, like the EU–U.S. Safe Harbor Agreement, is contingent upon the FTC being able to regulate data security, particularly now that there are questions about the strength of the U.S. data-protection program.

Also, the U.S. system of regulating privacy is done in a patchwork manner, so there is no one great law that regulates data security across the United States. And what that does is it leaves a number of different gaps. And the only statutes that really—the only avenue by which we can provide a baseline of data protection in the United States right now is Section 5 of the FTC Act.

And so Section 5 helps harmonize a lot of data-security practices, and it also has been consistent with a lot of other data-security regulatory regimes.

Mr. CUMMINGS. You heard the testimony of Mr. Daugherty and Mr. Roesler—by the way, gentlemen, I am sorry that you have gone through what you have gone through. I spent my life representing people who were not properly—they were improperly accused.

But you heard their testimony. I was just wanting to get your reaction to that. It seems as if there is a question—and Mr. Stegmaier talked about this a bit—as to charging folks. The way that folks are charged, they use data that—I think, Mr. Stegmaier, you would agree with this, based upon what you just said—that might you consider unfair charging. Would that be a fair statement?

Mr. STEGMAIER. I am not sure I understood——

Mr. CUMMINGS. Okay.

Mr. STEGMAIER. —precisely the question, sir.

Mr. CUMMINGS. But you understand what I am saying, right, Mr. Hartzog?

Mr. HARTZOG. So I think that the allegations that have been brought up are that there is not enough notice given to companies and that they are expected to follow rules that they say they don't know what they are.

The answer that I would give to that is that the FTC uses a reasonableness test, and a reasonableness test for regulating data security is the most common way, if you look across regulatory regimes, to regulate data security. So the Gramm-Leach-Bliley Act and HIPAA and many State regimes, all of them use a reasonableness test.

And the way that you execute a reasonableness test is you defer to some other existing body of standards, right? And so, in this case, it is a complete deference to industry standards. The FTC ac-

tually doesn't create the standard at all. Rather, they say, what is industry doing? And there is a whole body of study, so there are whole industries and fields of study dedicated to what makes not just cutting-edge data security but just industry-standard data security and best practices. And that is what the FTC says you should look to to determine what the baseline is.

And so the FTC actually isn't unique in its regulatory approach. There are States and other statutory schemes that utilize very similar approaches.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Mr. DAUGHERTY. Can you explain to me, then, why the HIPAA and HHS is not coming after LabMD?

Mr. HARTZOG. I am sorry?

Mr. DAUGHERTY. Can you please explain then, if you are talking about industry standards—we are a medical facility. We are under HHS and HIPAA. They have not come after LabMD or cited anything.

Mr. HARTZOG. Well, I actually can't speculate as to why. There are lots of different reasons why claims are brought or not brought.

Chairman ISSA. It is a good question, but we probably won't have any more between witnesses——

Mr. DAUGHERTY. Sorry.

Chairman ISSA. —if you don't mind.

But I do want to clarify just two things very, very quickly. You said a body of jurisprudence. That would imply that there has been decisions at the district and then the appellate court. Are there any?

Mr. HARTZOG. Well, we do have a decision at the district-court level in the Wyndham case, but, actually, jurisprudence can come from a number of different sources. And primarily, in the case of the FTC, it comes from the complaints that they filed.

Chairman ISSA. Okay. So the consent decrees are a body of jurisprudence where they sue and settle, and you are calling that a body of jurisprudence. I just wanted to make sure that is what you were talking about.

Mr. HARTZOG. Well, not the consent decrees, but rather the complaints that indicate what the FTC considers to be an unfair and deceptive trade practice.

Chairman ISSA. Okay.

And only one more quick one for Mr. Daugherty and Mr. Roesler.

Were you given any safe haven or guidance by the FTC as to how you could, in fact, not fall under unfair practices at any time from the beginning until today, those so-called standards that Mr. Hartzog has said exist?

Mr. DAUGHERTY. Well, sir, thank you for that question, Chairman Issa.

No. As a matter of fact, I stated, and as further indicated in my written testimony, quite to the contrary. In briefs and in quotations from the FTC, they argue they don't need to promulgate rules or inform us of standards. And even their experts said that we should Google them.

And this is just not a way to regulate an American industry and economy, let alone the world of medicine.

Mr. ROESLER. My response would be that——

Chairman ISSA. Yes, of course.

Mr. ROESLER.—the communication that Open Door received from the FTC was one simple letter; it was a warning that we received from them. There was no other communication. And during that time, it was simply about a file being out, and they listed the file.

Chairman ISSA. So they just didn't pursue you, nor did they give you guidance on how to remedy.

Mr. ROESLER. That is my understanding.

Chairman ISSA. And did you have something else you want to follow up on?

Mr. CUMMINGS. Just to follow up on—a friendly follow-up on the chairman's question.

Mr. Hartzog, you just heard what they said. You talked about a body of jurisprudence, and here you have folks who are saying they had no idea what was going on. Can you react to that?

Is that a fair statement, gentlemen?

You didn't——

Mr. HARTZOG. I would actually say that it's not a fair statement, nor is the FTC unique in requiring, you know, a standard to which there is not, you know, to the utmost specificity, right?

So, for example, in tort law, you are expected to build products safely, but there is not a manual that you get when you start designing products that says, you know, here are the 130 steps that you can take to make a product safe, right? You actually look to industry standards, which is another thing that is relatively common. And that is the kind of evidence that is used to determine whether you are acting reasonably or not.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Chairman ISSA. I thank all of you.

I will tell you, as somebody who has set industry standards, sat as a chairman of a trade association, I understand that safe havens are critical, industry standards, if you live up to them, you are supposed to get a level of immunity, at least from persecution by your government. It doesn't seem like that exists here.

Mr. Mica?

Mr. MICA. Thank you, Mr. Chairman.

And, Mr. Daugherty, you had Lab Med?

Mr. DAUGHERTY. LabMD, sir.

Mr. MICA. Okay, LabMD.

And you had Open Door, Mr. Roesler?

Mr. ROESLER. That is correct.

Mr. MICA. Two different activities.

Now, were you first notified by FTC that there was some breach or some problem with your handling of data, Mr. Daugherty?

Mr. DAUGHERTY. We——

Mr. MICA. When did FTC notify you first?

Mr. DAUGHERTY. They sent us an 11-page letter starting the inquiry.

Mr. MICA. Before that, no?

Mr. DAUGHERTY. No, sir. We were just under HIPAA.

Mr. MICA. And before that, no with you.

I am just trying to look at what took place here. So you both are conducting your business or activities, and you both get calls from

this firm, Tiversa. And that was the first notice that you had from anyone that you had problems as far as data security.

Is that correct, Mr. Daugherty?

Chairman ISSA. And I would only ask one thing, that whenever you answer, make sure it is verbal. The clerk is not allowed to write down a head nod.

Mr. MICA. Yeah, nods don't count.

So, Mr. Daugherty?

Mr. DAUGHERTY. Yes——

Mr. MICA. When you first—I want to find out when you first found out from some outside source that there was some breach.

Mr. DAUGHERTY. The outside source, sir, was—the first one was Tiversa in May 2008, and then the——

Mr. MICA. And Mr. Roesler?

Mr. ROESLER. For Open Door, it was also Tiversa that notified us first.

Mr. MICA. Okay. And that firm told you that they had, I guess, been fishing or surfing, whatever the hell they did. And then did they offer to help remedy your situation, Mr. Daugherty?

Mr. DAUGHERTY. They—well, yes, sir. They would not——

Mr. MICA. What was the offer?

Mr. DAUGHERTY. The offer was——

Mr. MICA. How much an hour?

Mr. DAUGHERTY. $475 an hour, with a 4-hour minimum, no guarantee.

Mr. MICA. Mr. Roesler?

Mr. ROESLER. It was $475 an hour.

Mr. MICA. And, Mr. Daugherty, what did you tell them?

Mr. DAUGHERTY. I told them I was not interested until they gave me more information.

Mr. MICA. Okay.

And, Mr. Roesler, what did you tell them?

Mr. ROESLER. I didn't respond.

Mr. MICA. You didn't respond. Okay.

So, after your initial contacts, your first contact of the breach, then you were later notified by FTC that there was a problem, Mr. Daugherty?

Mr. DAUGHERTY. Well, we were called by——

Mr. MICA. It was subsequent.

Mr. DAUGHERTY. Later in 2008, we were told by Tiversa they were giving it to Federal Trade Commission, and then Federal Trade Commission contacted us 14 months later.

Mr. MICA. Uh-huh.

And Mr. Roesler?

Mr. ROESLER. Yes, afterwards. Uh-huh.

Mr. MICA. Yeah.

And we tend to believe that FTC was informed or got that information from that company. Would you assume the same thing, Mr. Daugherty?

Mr. DAUGHERTY. Yes, sir, I would.

Mr. MICA. What would you assume, Mr. Roesler? You gave it to them? You called them up and said, "We are doing this, and you ought to investigate us?"

Mr. ROESLER. Excuse me?

Mr. MICA. I am just—that was a joke.

Mr. ROESLER. All right. Thank you.

So I don't know. I don't know the answer to that question. If that is how——

Mr. MICA. But somehow they got the data.

Mr. ROESLER. That is correct.

Mr. MICA. Well, to me, it looks like a little bit of an extortion game from a company trying to make a few bucks off of you guys, fishing and then coming after you. That is just my assumption. Now, we don't have FTC and others in here. We will have to find out more of what took place.

Part of this is that, you know, FTC was set up for a good and noble purpose, and that is to deal with deceptive and unfair trade practices. And we should have the right, too, to have whistle-blowers give them information. But a lot of the discussions also went around the standards and what is fair. But the standards do not exist specifically, Mr. Hartzog, as part of the testimony. That is first.

And then, secondly, you made a good point, that we don't want to clip FTC's wings to inhibit their power to go after bad actors. Is that correct?

Mr. HARTZOG. Yes, that is correct.

Mr. MICA. But if we find out, again, that the motivation for this was their nonparticipation in this scheme, it doesn't seem like they were treated fairly, one, and, two, that you two were never given notice to correct the practice. Were you given notice to correct what they considered——

Mr. DAUGHERTY. Oh, we were just given endless questions for years and then a suit. No. That was all we were given.

Mr. MICA. Were you given a remedial course or——

Mr. ROESLER. In our letter, it was suggested that we——

Mr. MICA. Cease and desist?

Mr. ROESLER. Something like that.

Mr. MICA. Remedy your situation?

Mr. ROESLER. That is right. Look into it.

Mr. MICA. Uh-huh. Because I think, again, businesses need to be notified by the regulatory agencies if there is a practice, and then if they don't clean their act up—you didn't devise those software systems, it was probably something you purchased, that had a——

Mr. DAUGHERTY. LimeWire was never even purchased. That is just malware that was out there——

Mr. MICA. Uh-huh.

Mr. DAUGHERTY. —that was put in by an employee with a total lack of authorization.

Mr. MICA. But it wasn't a purposeful thing, and when you found out, you tried to remedy it.

Mr. DAUGHERTY. Absolutely, sir.

Mr. MICA. Mr. Roesler?

Mr. ROESLER. We never had any evidence of having——

Mr. MICA. But when you found out, did you try to remedy it, the situation?

Mr. ROESLER. We just researched to find that we had no risk of that. That was——

Mr. MICA. Okay. All right.

I yield back.

Chairman ISSA. Okay. Thank you.

Mr. Hartzog, just to make sure, was LimeWire ever gone after by the FTC for their deceptive practices of creating the vulnerabilities?

Mr. HARTZOG. I——

Chairman ISSA. You have looked through the body of jurisprudence.

Mr. HARTZOG. I do not believe so, so I——

Chairman ISSA. But they never went after the people who created the vulnerability, just people who were victims.

Mr. HARTZOG. Yeah, I don't—I am not privy to investigations. I only know about the filed complaints. But as far as I know, there was no filed complaint against LimeWire.

Chairman ISSA. Yeah. That makes sense. They were probably without deep pockets and too slippery.

The gentleman from Massachusetts, Mr. Tierney.

Mr. TIERNEY. Thank you.

Mr. Hartzog, apparently there was ultimately an agreement or a decision that the companies that are testifying here today did not live up to industry standards or some other measure of reasonableness. Is that fair to say?

Mr. HARTZOG. Yes, that is fair.

Mr. TIERNEY. All right. So in that determination by the FTC of whether or not they complied with the reasonableness on that, is the sophistication of the company, the size of the company, the resources the company might have for establishing secure IT, the danger of the release of their data, are all of those factors in that determination of reasonableness?

Mr. HARTZOG. Absolutely. That is one of the reasons why a one-size-fits-all checklist for data security will never work, because it is far too dependent upon variables like that. And so, of course, large companies, large tech companies—you know, Microsoft and Amazon and all these others—are expected to have significantly different and probably more robust data-security practices than, say, smaller businesses. Now, of course, there is a baseline for everyone collecting personal information, but it varies wildly as to what is constituted in any given circumstance.

Mr. TIERNEY. So is there an FTC process where, when they become notified that a problem may exist, they notify the individual and give them an opportunity to cure?

Mr. HARTZOG. Because I am not privy to a lot of the internal investigations within the FTC, I am unable to answer that question.

Mr. TIERNEY. Mr. Stegmaier, do you have any information on that, whether or not the FTC as a matter of course, when they have an allegation or a concern that somebody may not be being reasonable in securing their IT, they give that company an opportunity to cure before they take action?

Mr. STEGMAIER. I have never had an experience in 13 years of doing this where they proffer the opportunity to cure in the manner that I think you are suggesting.

I have had a number of nonpublic resolutions, many, many times. But I haven't had this sort of, I think in the chairman's words, safe-harbor situation where they say, "We have brought this

to your attention, we see that you have taken corrective measures, and we have determined that that, you know, is in fact good enough." In fact, it is their practice, in part of Mr. Hartzog's analysis, that the agency doesn't typically issue what would be referred to as a closing letter for investigations.

But in my, you know, private, personal capacity appearing before the agency representing clients, the characterization you described is not consistent with my experience.

Mr. TIERNEY. Are either Mr. Hartzog or Mr. Stegmaier familiar with a situation where their clients were notified, as Mr. Roesler was, that you apparently have a problem and then no further action was taken because your client did something about it?

Mr. STEGMAIER. So it hasn't been my experience that the agency is typically calling to the attention of individual companies incidents or situations, but, rather, they come, investigation in hand, with an investigatory posture, trying to figure out what happened, rather than more a notice and corrective posture.

But, to be clear, I am aware of numerous cases where the agency has chosen not to continue investigating.

Mr. TIERNEY. Okay.

Is that similar to your information, Mr. Hartzog?

Mr. HARTZOG. That's correct, based on my information.

Mr. TIERNEY. Thank you.

Mr. Roesler, you received a letter from the FTC notifying you that they believed you had an issue and suggesting that you do something about it.

Mr. ROESLER. That's correct.

Mr. TIERNEY. All right. And what you did about it, you said, was you went and rechecked again to see if your people could find anything on the peer-to-peer; is that right?

Mr. ROESLER. What I said was that our IT subcontractor looked at our network to see if there was any P2P software within our network or on any of our computer laptops, any work stations.

Mr. TIERNEY. Did you at all do any research or ask your legal counsel, your IT subcontractor, to do some research about what the best practices in your industry were and whether or not you were, in fact, complying with those?

Mr. ROESLER. Indeed, we did.

Mr. TIERNEY. And what was the result of that?

Mr. ROESLER. The result was that we were meeting those standards, our network was secure, and that we were compliant.

Mr. TIERNEY. And did the FTC ever take any follow-up action against you?

Mr. ROESLER. None that I am aware of.

Mr. TIERNEY. Thank you.

Mr. Stegmaier and Mr. Hartzog, again, your help, if you would. When a determination is made by the FTC that there is noncompliance or that there is an unfair or deceptive practice, are the penalties automatic, set at a certain amount once it is found? Or is there discretion for the FTC to take into consideration mitigating factors?

Mr. STEGMAIER. So the agency doesn't actually have statutory penalty authority. They enter into a consent decree, which typically doesn't have a monetary penalty or a remedy.

As to the factors that they use in terms of how they decide which cases to prosecute or which cases not to prosecute, I would respectfully disagree with Mr. Hartzog in the sense that, having done this for a long, long time, the precise motivations and contours of what constitutes reasonable behavior and reasonable information-security behavior from the perspective of the agency that's authoritative is no more clear to me today than it was 13 years ago.

Mr. TIERNEY. I am going to let you guys fight that out offline here on that.

So if there's not a monetary penalty, what is the nature of the action that the FTC takes ultimately?

Mr. STEGMAIER. I think one way to think about it is to have a new board member who helps supervise your privacy and data-security process for the next 20 years, including, typically, biennial privacy and data-security audits through an approved third-party contractor who essentially will, you know, audit and review your processes and report to the agency.

Additionally, they have a tool which they call—is commonly referred to as fencing-in relief, through which, once you're under an order, you are subject to financial penalties if you should violate the order. And, in my experience, it's not uncommon for companies to spend as much as a half-a-million dollars a year or more simply to undertake to comply with the underlying orders.

So I would respectfully disagree with Mr. Hartzog to the extent that it takes into account the nature and size of the underlying companies. In fact, my experience has been the opposite, that the size of the company doesn't dictate what level of security the agency seems to believe is required in a number of instances.

Mr. TIERNEY. And I assume that——

Chairman ISSA. The gentleman's time has expired.

Mr. TIERNEY. Can I ask unanimous consent for one further question?

Chairman ISSA. As long as it doesn't take another minute and a half extra, go ahead.

Mr. TIERNEY. I'll do my best.

And the cost of this, sort of, outside entity or auditor that you're talking about is borne by whom?

Mr. STEGMAIER. Entirely by the company, sir.

Mr. TIERNEY. Thank you.

Chairman ISSA. Thank you.

Mr. Walberg.

Mr. WALBERG. Thank you, Mr. Chairman.

And thanks to the witnesses for being here.

Mr. Stegmaier, if you could just further help me to understand, what are the FTCstandards for determining whether or not a company's data-security practices violate Section 5?

Mr. STEGMAIER. Thank you very much, sir.

A couple of things. The articulated standard is one of reasonableness, and that is the extent of the standard.

I note that for the folks that are here today—and I think this is important for the committee to understand—I think that we learned from Mr. Roesler and Mr. Daugherty that there were initially begun investigated—the investigation in 2008. It wasn't until 2011 that the Federal Trade Commission issued a best-practices

guide identifying a number of recommendations that it thinks are required for reasonable security.

But to answer your question I think more directly, the troubling thing about that guide and the thing that has been difficult for many companies is, if you asked me to identify which, if any, of those items that they identify as best practices are legally required, I could not tell you.

Mr. WALBERG. So this is an evolving notion, as it were.

Mr. STEGMAIER. Absolutely. And I think the agency itself has taken that position repeatedly. The agency takes the position that it needs flexibility because technology is changing, what we think is privacy is changing, data security is changing.

Mr. WALBERG. Well, what, then, gives the FTC the authority to take enforcement on these evolving actions, especially in what's considered reasonable?

Mr. STEGMAIER. Sure. So, as Mr. Hartzog identified, the language of Section 5 is incredibly broad, and courts have generally given deference under what's known as the Chevron deference—Chevron case to agencies to determine their own jurisdiction. So, unless that exercise of jurisdiction is arbitrary or capricious, for the most part, absent Congress stepping in, the agency's determination, you know, will prevail unless or if a court disagrees.

And, as I mentioned to the chairman earlier, there are a number of cases pending that challenge exactly this question.

Mr. WALBERG. Mr. Hartzog, do you agree or disagree that the FTC should be taking the lead in establishing new regulations governing data-security practices?

Mr. HARTZOG. Well, I think that the FTC certainly plays the pivotal role and should play the pivotal role in establishing data-security regulation in the United States, but I do think that it's wise for the FTC to continue to defer to industry standards rather than try to make up their own standards, but, rather, follow what industry has determined is reasonable and appropriate data security. Because I think that that kind of deference keeps the FTC from acting in an arbitrary or inconsistent way.

Mr. WALBERG. So, in other words, kind of a shared partnership lead?

Mr. HARTZOG. That's right. So it's a co-regulatory regime, right, where you let industry say this is what is reasonable in our field, and then the FTC then looks to that to determine which companies have gone beyond the boundaries of reasonableness.

Mr. WALBERG. Mr. Stegmaier, can a business owner look up the rules for data security to make sure a business is in compliance?

Mr. STEGMAIER. So if you're subject to the Health Insurance Portability and Accountability Act, you can. In fact, the HHS has issued privacy and data-security regulations. The Federal Trade Commission has not.

If you are a financial institution subject to the Gramm-Leach-Bliley Act, there has been notice-and-comment rulemaking; you can look up those regulations. But, again, if you're subject to the FTC's jurisdiction——

Mr. WALBERG. You can't.

Mr. STEGMAIER. —you cannot.

Mr. WALBERG. A pattern is emerging.

Mr. Daugherty, did you know where to look up the rules or informal policies that governed FTC data-security practices before you were contacted by FTC?

Mr. DAUGHERTY. No, sir, because there were none. I mean, we've had professionals in and out. We had Stanson's two people in. No one said anything about them. We were fully within the medical community.

Mr. WALBERG. How easy or difficult is it to keep up with these informal policies?

Mr. DAUGHERTY. Well, I think it's nearly impossible, I mean, because they don't tell you till after the fact, whereas in HHS, in the world that we reside, in a regulatory world, it's quite simple. But in, you know, the world of medicine, which they're trying to get into, they're not using that format.

Mr. WALBERG. And, finally, Mr. Daugherty, in your opinion, is it fair for the FTC to expect businesses like yours to be able to locate and follow data-security practices?

Mr. DAUGHERTY. Oh, we're all for following data-security practices, absolutely. But we need to, obviously, have them take a leadership role and not a reactionary role.

As much as they want to say how broad this needs to be, breadth does not mean infinity, and there have to be some boundaries. And they seem to continually argue, well, we have broad scope, we need broad scope. But that doesn't mean they don't have to say anything. I mean, we all have laws. That doesn't mean we call it a crime when we see it.

So I think they need to be more reasonable in their boundaries and their communications, especially when they choose to get into medicine. That is really an alarming overreach.

Mr. WALBERG. Sounds reasonable. Thank you.

My time has expired.

Mr. BENTIVOLIO. [Presiding.] The chair recognizes the gentleman from Massachusetts, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman.

Now, this dispute is currently in the FTC administrative court; is that correct?

Mr. DAUGHERTY. Is this to me?

Mr. LYNCH. Yeah, anybody.

Mr. DAUGHERTY. Okay. Yes, sir, against LabMD, yes it's in administrative court, sir.

Mr. LYNCH. It seems to me that's a good place for it. I don't understand how this matter—there are a lot of, you know, administrative disputes that one side or the other feels offended by. It just surprises me that you're before Congress, given the small amount of work we do anyway, and now we're engaging in this. I just—I don't think this whole dispute, this whole hearing is appropriately before us. Let me just get that out of the way.

Earlier, Mr. Hartzog and Mr. Stegmaier, we heard the chairman say that—and get confirmation from two of the witnesses that there is no breach unless someone uses the information that's been put out there. In other words, you can have a door that's unlocked, I guess is the analogy that was used, and that even though information was not kept secure, there's no breach until somebody actually uses that information that's been put out there.

Is that the state of the law?

Mr. STEGMAIER. So, whether or not a security breach exists is actually a term of art. As the members of the committee may be aware, I think at least 47 States have breach notification laws using differing standards or requirements. So I think we'd have to think about, sort of, a particular——

Mr. LYNCH. Well, let me ask you, do any of those States say that the information has to be used before a breach is declared?

Mr. STEGMAIER. They tend to use the operative phrases, acquired or accessed without authorization.

Mr. LYNCH. Okay. So just putting the information out on the Internet, if nobody is using it, there's no breach?

Mr. STEGMAIER. It's an active matter of dispute as to whether the mere accessibility of information constitutes a security breach, and a lot of really smart people would disagree very vigorously.

Mr. LYNCH. Yeah. So you can put stuff out on the Internet, secure information on the Internet, and that wouldn't be a breach, Mr. Stegmaier.

Mr. STEGMAIER. That's not what I am saying at all. What I'm saying is——

Mr. LYNCH. Okay.

Mr. STEGMAIER. —smart people would disagree, and they frequently and regularly do.

But I think an important consideration is, under HIPAA, for example, whether you adhere to the security rule—in other words, whether your systems are, in fact, secure—is different than whether or not you've had a breach. So under HIPAA——

Mr. LYNCH. Well, I'm just asking you here whether it's required in order to be guilty of a security breach, whether someone has to use the information. That's what I'm asking you.

Mr. Hartzog, do you want to take a shot at this?

Mr. HARTZOG. Sure. The mere fact of a breach itself, actually, isn't a violation of any particular law, right? So there are a couple of points: One is the Section 5 defining an unfair trade practice as one that either causes harm or is likely to cause harm. You actually don't have to have any kind of breach or misuse in the first place.

Mr. LYNCH. Yeah.

Mr. HARTZOG. The second point is, the only harm that can come isn't necessarily one of, like, say, user ID theft, right, so mere exposure can constitute it.

And then the third thing to remember is that the wrongful actions here aren't that a breach occurred, right? A breach is really perhaps just a symptom of the problem, which is a failure to have good data-security practices. So regardless of whether the breach happened or whether it didn't happen, whether information was available or whether it wasn't available, all of that only really goes towards showing whether there were good, reasonable data-security practices or not. And that's really what we're looking for.

Mr. LYNCH. Right. That's the preventative aspect of this.

Mr. HARTZOG. Right.

Mr. LYNCH. If we had to wait till your Social Security was used by someone, you know, then——

Mr. HARTZOG. Correct.

Mr. LYNCH. —we would have to sit on our hands until somebody was abused, you know, somebody's information was acquired. And——

Mr. HARTZOG. Which is very difficult to show. And it's important to remember that data security is a probabilities game, right? So——

Mr. LYNCH. Right.

Mr. HARTZOG. —what you want to—there's no such thing as perfect data——

Mr. LYNCH. Let me just jump to this quick. Mr. Roesler, your clinic serves patients that may have HIV or AIDS; is that right?

Mr. ROESLER. That's correct.

Mr. LYNCH. Did the master list file have personal information about clients of the Open Door Clinic?

Mr. ROESLER. It did.

Mr. LYNCH. And about how many Open Door clients were listed in the master list file? Do you know?

Mr. ROESLER. About 150.

Mr. LYNCH. And the FTC wrote you that the clinic file master list was available to users on this peer-to-peer file-sharing network, right?

Mr. ROESLER. They did.

Mr. LYNCH. So the information was out there. So are you saying that the FTC was wrong to contact you on that? Is that part of your complaint?

Mr. ROESLER. Not at all. No.

Mr. LYNCH. Okay. Where did the—the FTC has not filed an enforcement action against you for that, right?

Mr. ROESLER. That's correct.

Mr. LYNCH. So wherein lies the overreach on the part of the FTC?

Mr. ROESLER. I am not aware of overreach.

Mr. LYNCH. Okay.

I'll yield back. Thank you.

Mr. BENTIVOLIO. The chair recognizes the gentleman from Tennessee, Mr. Duncan.

Mr. DUNCAN. Well, thank you, Mr. Chairman.

And I appreciate Chairman Issa calling this hearing because what I've heard thus far is very disturbing to me. I was presiding over the House until a few minutes ago, and so I didn't—I'm sorry, I didn't get to hear the testimony.

But if I understand this correctly, Mr. Daugherty, this Tiversa firm contacted you or your company and told you of possible problems and asked you to hire them at a rate of $475 an hour, and then when you declined to do so, they turned you into the FTC.

Mr. DAUGHERTY. That's correct. That was all in 2008.

Mr. DUNCAN. And then the FTC started pursuing you, taking action against you.

Mr. DAUGHERTY. That's correct.

Mr. DUNCAN. And I think I just was told that you're close to being out of business, or——

Mr. DAUGHERTY. The laboratory operations closed in January of this year because we've been completely sideswiped by this.

Mr. DUNCAN. And Mr.—is it "Roesler" or "Roesler"?

Mr. ROESLER. It's "Roesler."

Mr. DUNCAN. "Roesler." Mr. Roesler, your story is very similar, is that correct, except you're still in business?

Mr. ROESLER. I don't know that my story is similar. It's got its differences. Yes, we are still in business.

Mr. DUNCAN. But you were contacted by Tiversa——

Mr. ROESLER. That's correct.

Mr. DUNCAN. —and for $475 an hour they would take care of your problems?

Mr. ROESLER. That's also correct.

Mr. DUNCAN. And then when you declined, they contacted the FTC.

Mr. ROESLER. That I'm not aware.

Mr. DUNCAN. Well, according to the staff briefing we have, the FTC—this Tiversa company told on or reported or turned almost 100 companies into the FTC.

And, Mr. Hartzog, don't you think that, in light of what's come out here today, that the FTC should check on something like this, if another private company turns in a company, to see what conflict of interest is present? Because there certainly was a conflict of interest in these cases we're hearing about.

Mr. HARTZOG. It's difficult for me to speculate on that without knowing the exact details. But it's my understanding that the FTC actually gets information about what constitutes, you know, a potentially unfair or deceptive trade practice from lots of different sources, including public complaints in general, many of which might be valid and many of which might actually be invalid. And——

Mr. DUNCAN. Well, I know they get them from many sources, but when there's an obvious seemingly almost criminal conflict of interest involved, it looks like the FTC would at least check that out. Because that could easily be checked out on the front end of things.

Mr. HARTZOG. Well, certainly, the FTC should make sure that any allegation that's turned into them is actually valid. And so I think that, of course, it's incumbent upon them to make sure that the facts that are alleged to them are actually true.

Mr. DUNCAN. Mr. Stegmaier, you're a law professor. Do you think anyone should be prosecuted criminally on things like this, what you've heard here today?

Mr. STEGMAIER. If the facts as alleged turn out to be true, no, I would not think that prosecution should necessarily be appropriate. But I think if I'm understanding your question more correctly, do I think it's appropriate for this committee and Congress to review the agency's behavior, I think it's incumbent on Congress to do so.

Mr. DUNCAN. What do you think should be done in addition to this committee looking into it?

Mr. STEGMAIER. So I don't profess to be an expert on all of the remedies or different, you know, mechanisms. But one of the things that I think we've seen and I think is, you know, critically relevant is to create an environment where companies can understand what's actually expected of them as a matter of law so that then when and if the agency should come to investigate them there's much less of an element of surprise. And that's really sort of the

crux, right? The Constitution protects us from being prosecuted when we couldn't possibly have known what the law is.

And I think Mr. Daugherty could testify or would testify about his experience in that regard, and I think he has testified to the effect that he understood that he was subject to HHS's jurisdiction. And being subject to the FTC's jurisdiction and then what that meant in terms of what's actually required is as opaque today as it was in 2008 for him.

Mr. DUNCAN. Well, the problem that many of us see now is that the Federal Government is prosecuting people for unintentional violations of the law. And that's not supposed to be criminal, but a zealous prosecutor can make an innocent, unintentional violation of the law seem to be criminal, and that's a pretty dangerous thing.

The government should be in the business of trying to help companies stay in business, not with the goal of trying to run people out of business, unless they have definite proof of intentional efforts to defraud people.

Thank you very much, Mr. Chairman.

Mr. BENTIVOLIO. The chair recognizes the gentleman from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman.

And welcome to our panel, especially my constituent, Mr. Stegmaier, who's obviously cogent, astute, perspicacious, very compelling testimony. And we're not surprised, coming from the 11th Congressional District of Virginia.

Mr. STEGMAIER. Thank you, sir.

Mr. CONNOLLY. Mr. Stegmaier, I wanted to clarify something you testified to just now. What is the status of Mr. Daugherty's case before the FTC?

Mr. STEGMAIER. So I haven't been following the precise contours of the case other than the existence of the administrative procedure is highly, highly unusual. I'm not aware of any other case that's actually used that procedure.

Mr. CONNOLLY. Mr. Daugherty, what is the status of your case?

Mr. DAUGHERTY. The case is on pause until the immunity decision and proffer is worked out with this committee. And then the judge will make a decision from that point.

Mr. CONNOLLY. Okay. So it's still in adjudication. Pending.

Mr. DAUGHERTY. Pending.

Mr. CONNOLLY. But there's been no verdict delivered or——

Mr. DAUGHERTY. No. This is correct.

Mr. CONNOLLY. Well, I will say I share some of—more than some of the misgiving of my colleague from Massachusetts, Mr. Lynch, about the appropriateness of this committee even the perception of intervening in the midst of, you know, a regulatory adjudication, for fear that, you know, we start to set a precedent. So anybody, you know, who doesn't like a procedure can just come here and we'll have a hearing and judge it for ourselves. I just think that's a dangerous precedent if that, indeed, is what's going on.

Mr. Stegmaier, the title of this hearing is "FTC Section 5 Authority: Prosecutor, Judge, and Jury." Do you view the FTC as playing a role as prosecutor, judge, and jury?

Mr. STEGMAIER. Absolutely. I think the structure of the administrative state, Section 5 being very broadly worded, with the agency

getting deference to its own determinations about its jurisdiction, as well as its interpretations of the law being plausible, absolutely create a situation where it is difficult, if not impossible, to create due process remedies or ways for review that most regular people would think our system of justice entitles them to.

And with respect, Mr. Connolly, to your comments about this particular proceeding, one of the things that strikes me is that, with respect to the fair notice doctrine and due process generally, if not here, where else? And I think that really begs the question. You know, in other words, Mr. Daugherty, I am not sure has any other place that he could go unless and until this proceeding is resolved.

So, you know, again, maybe I'm a bit of, you know, sort of a sentimentalist, but I think the due process concerns here are so significant that I would be, you know, troubled to wonder where else one might go for redress.

Mr. CONNOLLY. That sounds good, Mr. Stegmaier, but we cannot be substituting ourselves for regulatory agencies in the midst of their administrative procedures. The precedent that sets is very dangerous, in my opinion.

And, by the way, if there were thousands of them, there's no way you could raise the expectation that, no, no, this is where you come for redress if you don't like the process. Though, I am not disagreeing with you about the fact that there may be way too much authority, frankly, vested in this process. And that's a legislative issue, but not an adjudication.

Mr. Hartzog, would you respond to what Mr. Stegmaier said? Didn't he make a pretty good point there?

Mr. HARTZOG. Sure. No, so I would actually disagree. I mean, I agree in the sense that, you know, this kind of title of "judge, jury, and executioner" is—the FTC is not unique among administrative agencies in that it has been given enforcement power and the power to kind of dictate rules. That's actually kind of administrative law generally, right? So, to the extent that the FTC has the power to enforce the law and create rules through case-by-case adjudication, the FTC seems to be hardly unique in that respect.

With respect to, kind of, fair notice, due process concerns——

Mr. CONNOLLY. Well, can I just interrupt you there? Mr. Daugherty has a blog in which he refers to the FTC as "lying, cheating, breaking every rule in the book." "All professional tyrants and bullies have plenty of tricks up their sleeves. This nest," presumably the FTC, "is no exception."

So Mr. Daugherty——

Chairman ISSA. [Presiding.] Would the gentleman yield?

Mr. CONNOLLY. Of course.

Chairman ISSA. I think many Members on your side of the aisle have said the same about me on the dais. These allegations are not unique, are they?

Mr. CONNOLLY. Yeah, but I don't know if we all have blogs.

But, I mean, putting a charitable interpretation on what clearly is a source of anger and frustration for Mr. Daugherty is a sense of: I am not being treated fairly. This process is far beyond just a routine administrative process. It is one that, you know, is all-encompassing and all-powerful and capricious. My word, not his.

So is this just like any other administrative process? Is there something unique or different about this one? I'm not referring to the particular case; I'm talking about the process. Because you just said, well, it's hardly unique. But if I read this blog and only rely on it for witness to the FTC process, I might conclude it most certainly is different and unique, or at least I hope it would be, if this is accurate.

Mr. HARTZOG. Well, I can't comment as to the factual specifics. My——

Mr. CONNOLLY. I'm not asking you to.

Mr. HARTZOG. Right, right. So without knowing the internal deliberations of what happened with respect to the FTC investigation with this particular case, I will say if you look at the complaint that was filed in this case, it is very consistent with all of the other FTC data-security complaints. The FTC has been regulating data security since the late 1990s, and they've done so in a very conservative and incremental manner. The language that they employ is very consistent across every single complaint. The language that they use in their consent orders is very consistent.

And so if you look at the complaint that was filed in this case, it does, indeed, look very similar to lots of other complaints filed by the FTC. And so, in that regard, this is, you know, just another, kind of, incremental iteration on the FTC's data-security regulations.

Mr. CONNOLLY. And just a final point, if I may, Mr. Chairman.

Do you agree with Mr. Stegmaier that, if not here, where, that this is a place to come for redress if you feel you're not getting it in the administrative law review—I mean, the administrative judicial process?

Mr. HARTZOG. Well, I would just call note to the fact that everyone that is subjected to an FTC complaint has the right to judicial review. And so, you know, that seems to be the structure that was put in place precisely to put a check on administrative agencies.

Chairman ISSA. Would the gentleman yield?

Mr. CONNOLLY. Of course.

Chairman ISSA. Just for a short colloquy. I think you made an assertion that perhaps this hearing and our what you called "intervening" with the FTC was inappropriate. I just want to go through a couple of things very quickly for our benefit.

Have you had a chance to look at any of the proffer material brought to the committee voluntarily by a whistleblower?

Mr. CONNOLLY. I'm not sure what the chairman is referring to. I've looked at a lot of material.

Chairman ISSA. No, no. There was a proffer brought. The committee staff has reviewed some of it. There was a whistleblower who came to us, unrelated. We did not initiate it, but rather a whistleblower came to us. And that, in combination—and perhaps your staff can arrange—at the beginning, I asked everyone to look at the proffer. It goes more than an hour.

But, additionally, the reason that this committee feels that, notwithstanding an ongoing—many-year ongoing FTC activity, that, in fact, because Mr. Boback testified before this committee twice while he was, in fact, turning people into the FTC for eventual prosecution, and because a whistleblower came to us, and because that

whistleblower took the Fifth at the—asserted his Fifth Amendment rights at that proceeding, my understanding is the administrative law judge has for the time being held up, with no prejudice whatsoever, his proceeding as we continue to try to go forward.

The judge is able to go forward with the case at any time, of course, but both this chairman believes that we should hear the testimony of the whistleblower here and I think the FTC would like to hear the testimony of that individual because, since he was a prior employee of Tiversa, he is, in fact, likely to be a fact witness as to whether or not there is credible evidence against Mr. Daugherty's company, which, by the way, doesn't go to the FTC's authority that we're discussing here today. It really goes to the question of, is the FTC accurate in one or more of its pleadings?

And for the gentleman's edification, it is our opinion that, at a minimum, if the assertions that have been made are true, the FTC has been misled and this committee has been misled on multiple occasions. The Secret Service, NCIS, the White House, through the assertion made—and I don't know if the gentleman was here when it was made, but the assertion that Marine One's cockpit upgrade was compromised when it was in Iran may not have been true. All of those things caused this committee to think that we need to act now and to look into it.

But I appreciate the gentleman's rightful statement that it's not for us to second-guess the FTC. Their administrative law judge has to make their own decision. We also, though, believe that we have an independent obligation based on the things I outlined, and I would hope the gentleman would agree.

Mr. CONNOLLY. Mr. Chairman, it might surprise you to hear that, in some measure, I do agree. However, I guess I'm raising the question, not for a solution here, about, what are the right boundaries for us, and when do we properly intervene because of our oversight function and duty?

I was asked before this hearing, you know, do we have a role to play in oversight of FTC, and my answer was absolutely. And if there's, you know, something to be reformed or something certainly to be looked at, that is absolutely a proper function of this committee. And the idea that it's never proper is to be rejected.

However, there are boundaries. And when there's a specific case in front of a judge, I am concerned that it not even be construed as a perception that we are attempting to tilt the judgment in a particular way or to make ourselves the place of redress when people have a grievance, even though that grievance may very well be legitimate.

Our role is not to hear the case all over again. It is to try to, you know, ameliorate the grievance if there are legitimate aspects to it that can be addressed legislatively. That's what I was raising.

Chairman ISSA. And I think the gentleman and I would agree that we have to be very careful, both yesterday with the IRS and today with the FTC. But I do believe, when somebody has testified before this committee multiple times, the assertions may be incorrect, and, as a result, a series of suits already completed by the Federal Trade Commission with consent decrees might, in fact, have been flawed.

And, tangentially, Mr. Roesler, obviously, we are concerned that a pattern of activity, business practices, you may have been a victim of and suffered—you and your insurance company suffered distraction and cost for years. So we are concerned with it.

And that's why I was so appreciative of your being here today. This was a tough one for you to do. It's tough for you to tear yourself away and to take time out. But, hopefully, maybe a little bit like some hearings we've had over the years, where people don't understand them at the beginning of it, if, in fact, they come to some of the assertions being true, then at the end of it all people will say, yes, it was worthwhile.

If, Mr. Connolly, if, at the end of it all, whistleblower statements are wrong, assertions are wrong, and all of what we have been told is not true, and if, for example, that Pittsburgh event, the law firm was just a coincidence, if, in fact, both of these individuals had real breaches, then, in fact, if all those things be true, then, in fact, we went down a look-see that didn't end up. But today I believe very strongly and I think at least two of our witnesses feel strongly that there's at least a credible case to look into it.

And I might close—and I thank the gentleman for so much yielding. I remember when Pat Tillman's family was in front of this committee. I remember us looking at various events that were very controversial, assertions by grieving family members. This committee has taken the breadth of investigations by both sides' chairmen, and we have explored them. We explored steroids in baseball. We've done a number of things. The ranking member and I have continued to work on trying to clean up the NFL's problem with human growth hormones. Those are not within the mainstream.

So I do appreciate the gentleman. And I want to be very careful. I would ask, again, all Members to look at the proffer, to meet with the whistleblower. Even if he is never to be granted the opportunity to testify, the proffer itself might give you the reason for why we are going forward to try to find the facts through other means and why this hearing is here today.

Mr. CUMMINGS. Will the gentleman yield?

Chairman ISSA. Of course.

Mr. CUMMINGS. First of all, Mr. Chairman, you know, I was questioning as I was listening to Mr. Connolly whether this is, in fact, intervention. I'm not sure that it is, to be frank with you. But I'm hoping that, at the end of the day, that the FTC hears this. Clearly, there are some things that need to be resolved here.

And, you know, when I hear the stories of Mr. Daugherty, Mr. Roesler, I think it concerns all of us if you have been treated unfairly, because we try to fight against that kind of thing.

But, again, I think—and I'm glad you said what you said about being careful. Because it's interesting, in my office, Mr. Connolly, I tell my staff that if somebody walks in there and there's any kind of pending anything, judicial, quasi-judicial, I'm not touching it, I'm just not going to touch it, because I don't want to interfere.

Mr. CONNOLLY. Right.

Mr. CUMMINGS. And I think there's probably a problem with it anyway, ethically.

But, hopefully, this will lead to something where there's some clarification, Mr. Chairman, so that we don't have these kind of sit-

uations, or, if nothing else, at least some clarity comes to the people who are in the industry as to what is expected of them, what's fair, what's reasonable.

Mr. CUMMINGS. And if we can come to that—and, again, as I said a little bit earlier, Mr. Chairman, we have not said absolutely against immunity for a whistleblower. We just want to make sure that we dot our i's, cross our t's.

And so, thank you very much.

Chairman ISSA. I thank the ranking member, and I thank Mr. Connolly.

We now go to the very patient quasi-expert on HIPAA, Dr. Gosar.

Mr. GOSAR. Well, thank you, Chairman.

I'm a dentist before I came to Congress, so I'm very aware of HIPAA and OSHA, and it's very different from what I'm understanding here, Mr. Daugherty, right? I mean, we have classes, we have rules, regs. They're pretty astute and pretty well-defined, right?

Mr. DAUGHERTY. Yes, Congressman. As a matter of fact, we enjoy daily mailing offers for educational seminars that anyone could have at any day.

Mr. GOSAR. And so, like, a typical small business, you update, you try to keep up with trends, making sure that you're up to par in protecting databases, as well, true?

Mr. DAUGHERTY. Correct. We always had an IT staff of at least 3 people, even when we were only, like, 15 employees. And we also had an outside company help.

And, as a matter of fact, we upgraded to—we found in the small-business community and in the medical community that's under 100 or 200 employees, there were no security products out there. So when the FTC approached us, when we were trying to get an answer of what to do and we couldn't get an answer, we went out to the industry, and they didn't have products for us. They only were with 500-employee companies and up. So we had to find a company that would actually customize something for us that was built for someone bigger that would actually work with us, and we could only find two vendors to do it.

Mr. GOSAR. So, I want to get back to this fair notice. It seems like if what I heard from Mr. Hartzog in regards to looking across the industry for fair and applicable application, they should've taken some of that into consideration.

Mr. DAUGHERTY. Well, I would agree with that, sir, yes.

Mr. GOSAR. Yeah.

Mr. Hartzog, are you real familiar with why the FTC is even in business today? Do you understand the history from 1978 to 1980? In fact, my Democratic colleagues almost—actually shut them down during 1980.

Mr. HARTZOG. I——

Mr. GOSAR. And underneath, in regards to—the FTC only survived in its agreement to limit its discretion by issuing its now-revered unfairness policy statement, true?

Mr. HARTZOG. That's correct.

Mr. GOSAR. So there's even more onus—you bypassed it, but there's even more onus on the FTC to be fair and applicable across these applications. Would you agree?

Mr. HARTZOG. Yes. They are——

Mr. GOSAR. Well, I mean, so the statute and the mission is very specific to the FTC, right? So the application across all agency boards are not exactly what you said.

Mr. HARTZOG. Well, with respect to whether something constitutes an unfair trade practice. So it actually isn't even limited to deception, but the policy codification was to an unfair trade practice.

Mr. GOSAR. Well, my whole point is the FTC is further scrutinized by its jurisdiction in regards to that. So they were disciplined by Congress, okay?

Would you agree with that, Mr. Stegmaier?

Mr. STEGMAIER. I think the agency has more of a track record, historically, and speaking purely historically, of potentially running afoul and having congressional oversight. And, for example, their rulemaking authority is highly constrained coming out of some of the same things I believe you're talking about.

Mr. GOSAR. Yeah. So let me—I guess my question is, if we're coercing settlements, what good is the rule of law? How are we overseeing the FTC in a proper adjudication if they're already being scrutinized a little differently because of their past history?

Mr. STEGMAIER. I think it's a really good question, and I think it's one we need to explore further.

Certainly, having represented companies that felt they were being coerced, I very much sympathize with the tone and tenor of your statement. And, in the same breath, I would just say that my experience with the folks actually working at the agency has been of a really bright, hardworking, dedicated group of people that believe in what they're trying to do. And I think one of the things that can be happening here is a bit of disliking the messenger versus the message.

And part of that is simply because we, as a society, haven't resolved what privacy and data security mean, but we have a law enforcement agency that's out there prosecuting companies with what it thinks it means, you know, over more than a decade now. And that's really, I think, what brings us here, is a tough spot independent of anything that Mr. Daugherty or the other information before the committee or the proffer, none of which I'm specifically familiar with.

Mr. GOSAR. And it seems to me that we haven't had oversight or reauthorization of the FTC, and maybe we need a mission. I mean, just because you're bright and you're affable in your job, it doesn't make you right in your application of the law, does it, Mr. Stegmaier?

Mr. STEGMAIER. So I made a note to myself earlier: Just because you do something doesn't mean you have the authority to do it. And so I would agree that a measure of oversight and review is appropriate, given, as the agency acknowledges, that technology is moving very rapidly, data is moving very rapidly, and, clearly, the agency has a very important role to play, but that is one that is, you know, limited and subject to congressional review.

Mr. GOSAR. And so, would you still agree that the review of you're innocent until proven guilty?

Mr. STEGMAIER. I would agree that you are absolutely innocent until proven guilty. I think that's the entire reason why I'm here today.

And I think, more importantly, it's really a shame if you're prosecuted and you couldn't possibly have known what the legal requirement was for which you are being prosecuted. And that's what the fair notice doctrine is about in the articles I've written.

Mr. GOSAR. Yeah.

Mr. Hartzog, would you agree with that?

Mr. HARTZOG. I agree with the general statement, but I would also say that the case-by-case way of establishing law is actually a part of——

Mr. GOSAR. I mean, you didn't give a very good, I mean, notice about applicability across the board here. You tried to cite as an expert witness, and you tried to cite, which you really couldn't. And shouldn't that be more based upon predicated caselaw so we should see, instead of coerced settlements, we see more applicability going towards the courts?

Mr. HARTZOG. If I might, actually——

Chairman ISSA. The gentleman's time has expired, but you may answer.

Mr. HARTZOG. Thank you.

If you look at the complaints, actually, we actually see substantial overlap of the FTC complaints with the HIPAA security rule and Gramm-Leach-Bliley. And so, actually, it's actually a fairly nuanced standard. If you look at the complaints which, established in a case-by-case manner, really outline what an unfair or deceptive trade practice is.

Mr. GOSAR. Thank you.

Chairman ISSA. Thank you.

We now go to the gentlelady from Illinois, Ms. Duckworth.

Ms. DUCKWORTH. Thank you, Mr. Chairman.

Thank you, gentlemen, for being here today.

I just want to establish some clarification. And, Mr. Roesler, I know you do tremendous work in support of our citizens who are suffering from AIDS and do everything that you can through your organization to support your clients.

I just want to, sort of, go through the timeline of your particular instance. You were contacted by Tiversa saying that they had these files that they had found on peer-to-peer networks and that for a certain amount of money they could help you with it. Subsequent to that, you then went to your IT providers and did a thorough search and determined that nothing in your networks had been breached. Is that correct?

Mr. ROESLER. That is correct.

Ms. DUCKWORTH. And, at a later point in time, you received a letter from the FTC saying that there was this file in the Internet, and it was a different file name from the file that Tiversa had informed you was out there. Is that correct?

Mr. ROESLER. That's also correct.

Ms. DUCKWORTH. Great.

Prior to this time, did you not suffer a break-in to your facilities, where a laptop was physically stolen from your facility?

Mr. ROESLER. That's correct. In 2007, Open Door was the victim of a theft of one of our laptops in our Aurora clinic space.

Ms. DUCKWORTH. Correct. And you did report that crime to the police?

Mr. ROESLER. That was reported, yes.

Ms. DUCKWORTH. Yes.

So when you got the notice from FTC with a different file and in going back and reviewing, is it true that you have determined that these files that were on the Internet were not a result of any type of a security breach to your network but probably came from that laptop that was stolen?

Mr. ROESLER. That is an assumption that we do have, that the laptop that was stolen had these as well as other documents on that computer.

Ms. DUCKWORTH. And so the FTC has not pursued—has not contacted you other than that first letter to say they found these files on the Internet, this is a warning, you need to deal with it. Is that correct?

Mr. ROESLER. That is correct. Thank you.

Ms. DUCKWORTH. Okay.

Do you have any evidence that the FTC turned over information of any of those files to any law firm that then initiated the class action lawsuit against you?

Mr. ROESLER. No evidence at all.

Ms. DUCKWORTH. No evidence at all.

So what I'm trying to get to here is the fact that there are two different things going on. There are the practices, which I think appear to be very egregious, on the part of Tiversa, which I want to get to the bottom of, and then the fact that you were very much a victim of an actual theft to a facility that probably did have a lock on your front door, quite literally, and then the FTC finding a different file on the Internet from the one Tiversa contacted you with and said, hey, this file is out there, take a look at it. You dealt with it.

The only thing that I'm somewhat concerned with in terms of your actions is that you did not notify your clients for over a year whose names were on that stolen laptop. Is that correct?

Mr. ROESLER. That is correct.

Ms. DUCKWORTH. But that's a matter for State law; that's not under the jurisdiction of this committee here.

But you've settled the lawsuit with this law firm, wherever they got the information from, not from the FTC but from somewhere else. Your clients—many of whom are back with you and are happy with the treatment that they're getting?

Mr. ROESLER. That's correct. We are back to doing business as usual.

Ms. DUCKWORTH. Which you love, which is taking care of your clients.

Mr. ROESLER. Very much. Thank you.

Ms. DUCKWORTH. Thank you.

Mr. Hartzog, could you give me your opinion on, was it appropriate for the FTC to contact Mr. Roesler to say that, hey, we found a file on the Internet that contains your clients' names?

Mr. HARTZOG. Sure, in the sense that the FTC has, you know, a broad ability to look into lots of different data breaches to determine whether there was reasonable data security or not.

Chairman ISSA. Would the gentlelady yield just for a point of information?

Ms. DUCKWORTH. Yes, I'll yield.

Chairman ISSA. The committee can provide you with the produced written data that shows that Tiversa provided that information to the FTC. So the source in both cases was Tiversa directly in contact and then indirectly when the FTC gained from Tiversa that same information that Open Door failed to, if you will, pay for protecting.

Ms. DUCKWORTH. Thank you, Mr. Chairman. But I do think the FTC did contact Mr. Roesler with a different file name.

Which is how I believe you were able to come to the conclusion or the assumption, a working hypothesis, as it were, that it likely came from this laptop and not from a breach of your network.

Mr. ROESLER. Okay, no, that's not exactly correct.

Ms. DUCKWORTH. Okay.

Mr. ROESLER. So during the litigation and during discovery, the law firm was able to produce quite a few documents that had been downloaded from a peer-to-peer network. It was when we started looking through the piles of documents that we were able to ascertain what the likelihood is of which employee might have been producing most of those documents. And from there, we were able to then figure a timeline that, well, this employee doesn't currently have these documents on their current laptop; however, come to think of it, 2 years ago, their laptop had been stolen out of our clinic. And that's when we started moving backwards in that thought process.

Ms. DUCKWORTH. Okay. Thank you.

I'm out of time, Mr. Chairman.

Chairman ISSA. Thank you. If the gentlelady would just allow me to follow up on your line?

Mr. Roesler, do you believe that Tiversa provided you with all the information and all the files that they had found?

Mr. ROESLER. Could you repeat that question?

Chairman ISSA. In other words, when they approached you and said, we found this vulnerability, do you believe at that time they provided you with a sample of what they had found or all of it so that you could figure out the source?

Mr. ROESLER. Thank you, Chairman. That's a very good question.

They produced one document, what I believe to be—it is my opinion, but that they had more than the one that they described to us that they had at the time.

Chairman ISSA. And I'll go to the ranking member in just a second.

The reason I want to do that is Ms. Duckworth's two different documents. Since our data that's been found in discovery shows that Tiversa did turn over to the FTC the documents, or that we have a list with your name and so on on it, it appears as though

what FTC brought you, which was a different document, was also from the same source of Tiversa.

And, Ms. Duckworth, the reason—and I appreciate that you're talking in terms of looking at Tiversa and so on—is, as far as we can tell, the only taker of this personal identifiable information that we know for sure reached into his systems on his network and pulled out files was Tiversa, who reached in, pulled them out, and turned them over to the FTC. That's the part that we know, is that at least one company found the vulnerability, took the information, gave it at a minimum to the FTC. And there is some question by the committee as to how the law firm got that same list and produced a class action, a law firm in the same city.

And that's, I think, what the gentlelady is really looking at, is this doesn't look good. And the effects on Open Door were devastating.

Ms. DUCKWORTH. Well, I would agree with the chairman that the effects on Open Door was devastating, but I don't agree that they reached into their network. Open Door has determined that there was no breach of their network. And, in fact, the data breach came from a stolen laptop. So if Tiversa got this information, they got it from someone else who uploaded the information from a stolen laptop, 2 years prior, to the Internet.

It was not a breach of their network. They did a thorough search of their network. And, in fact, Tiversa is getting this information that someone else, presumably the thief who broke into their facilities and stole their laptop or someone that got that information off the laptop, uploaded. It's two different mechanisms——

Chairman ISSA. And I share with the gentlelady very much versions of that possibility. That laptop that was stolen could've had LimeWire added to it. It could've been put up on the thieves' Internet site, and Tiversa could have found it out on the Internet. The interesting thing was that Tiversa did not go to the laptop or to some other posting; they actually went to this company and said, we found the vulnerability on your site.

And that's what is so perplexing, is they didn't say, we found this information in the Internet. They went to Open Door and said, we found your vulnerability and we offer you services for your vulnerability. Now, my understanding is Tiversa also will talk about helping cleanse lost data, clean up what's been out there on the Internet. There's a lot of services people talk about.

But it is confusing that, in fact, this data, we know for sure, got into Tiversa's hands. And in our discovery, we do not yet know, did they really get it off of your Web site at Open Door? Did they get it off the stolen laptop?

One thing we're convinced about is that they may very well have never gotten it, seen it somewhere in the Internet, except on a vulnerability from a peer-to-peer. And, in fact, it may never have been made available so as to harm the 180-plus AIDS patients that in some measure felt offended and served a lawsuit.

Ms. DUCKWORTH. I would have to disagree with one portion of that, Mr. Chairman. I share your concern with Tiversa's very predatory practices, and I think we should look more into it and I would love to have them here. But I think, in this case, Tiversa said they found this data on a peer-to-peer network, not on Open

Door's network. They found it on a peer-to-peer network. That's what they told Open Door, "We found it on a peer-to-peer network."

Open Door then went in and looked at their peer-to-peer network and saw and confirmed that it had not been breached and that there was no vulnerability in their peer-to-peer network. Just because Tiversa found it on a peer-to-peer network does not mean that that peer-to-peer network belonged to Open Door. Someone else uploaded it from, likelihood, that stolen laptop to a different network.

So I just want to make sure that Tiversa is—they could possibly be trolling the Internet for this data on various peer-to-peer networks, not necessarily Open Secret's, found it, and then tried to get them to purchase services. So it's two different things. And I just want to make sure that this is—the things that Open Door has suffered has been because of Tiversa and Tiversa's actions with the law firm.

And, in fact, as far as the FTC is concerned, they sent them a note saying, there's this form out there—there's this file out there, you need to take a look at it. And they've not prosecuted, they've done nothing else. Really, they've been the victims of a class action lawsuit that was initiated by Tiversa after they found a document on a separate peer-to-peer network that was not the one that was Open Secret's—I mean, Open Door's.

Chairman ISSA. You may very well be right. And I think you're getting a nod from Open Door.

But I think the gentlelady has made the exact point that I hope we can all come together on, which is we have a whistleblower who wants to give us detailed information directly related to each of these events with actual recorded hard disk data and only asked that his involvement and his testimony as to how he was involved in this at Tiversa not lead to his prosecution. And that is all that, in fact, when you see the proffer, if you will please see it, video proffer, you're going to see, is a demonstration specifically of that. And it does give us a fact witness, however flawed in any other way, a fact witness who will make specific allegations as to particular companies and where their data was or wasn't; additionally, and for me as a former ranking member and member of this committee, is also prepared to testify about evidence that was presented to this committee under oath. And that's why we have sought to have this witness.

Today's hearing deals with what we know and what happened to these individuals and with some of the pitfalls of, does the FTC, for example, in the case of Open Door, did they get second corroboration or did they send that letter in your case, and a lawsuit in your case, based on a single source that may or may not have been accurate?

And, to a certain extent, I know we're all getting mired in Section 5 authority. This is more than Section 5 authority. It's about whether an agency, even if it has the authority, what are the safeguards before they file a lawsuit? What are the safeguards to make sure that the allegations are independently corroborated? Because cybersecurity is, in fact, as the gentlelady knows, it's not a hard science where you can be sure. And if somebody says this happened, making sure it happened is important.

So this is a broad subject. Cybersecurity is a core element of our oversight, not just here but throughout government. And it's one of the reasons I thought bringing up the whole question of how do we move cybersecurity positively—because, Mr. Hartzog, I think you would agree, and, Mr. Stegmaier, I think you would agree, that to the extent the FTC has authority, it's in order to protect against unfair practices, that's their basic—but, in fact, to move us into greater security and reliability of people's information when it's held by third parties. And that goes to the core of cybersecurity in and out of government.

So my view was this hearing, separate from the other discussion that I hope to have with the whistleblower, this hearing was worthwhile not because there's an ongoing investigation or case, Mr. Daugherty, and not because of what you've suffered alone, but because you're helping America understand this is complex, we have to make sure that allegations are correct, and we have to make sure that if there's a bad actor basically selling services in an unethical way that we hold them accountable.

And that's why I'm so interested in your line of questioning and I support it and I appreciate it.

Ms. DUCKWORTH. Thank you, Mr. Chairman.

Again, I don't think the FTC filed a lawsuit against Mr. Roesler, just warned him that the file was out there. But I agree with you that I would like to know more about this process, so it would be great if we could have the FTC here in testimony.

Chairman ISSA. And we do intend to. What we're asking is that they answer our questions as to some of this corroboration and so on. We expect to ask both Tiversa and the FTC.

One of the challenges—and I hope the ranking member will chime in on this, too. Mr. Connolly's statement about an ongoing lawsuit means that we have to think about how and when we bring the FTC in so that we not put them here specifically talking about a lawsuit that is ongoing. So I want to be a little careful on that. We are working with the IG. And the FTC's IG is available to come in and brief your office, because she has a separate investigation that we're respecting, her ongoing investigation.

Mr. Cummings?

Mr. CUMMINGS. Thank you.

Mr. Chairman, I want to just go back to something you just said.

And I want to direct this to you, Mr. Hartzog. When the chairman—and I think when you boil a lot of this down, this issue of independent corroboration and trying to be fair—and I think that's what the chairman is saying. He's not—I think he's saying that, you know, there may be appropriate times, but trying to have a sense of fairness with it all. Because these gentlemen, I think, would say that they feel that they have been treated unfairly.

So can you talk about, I mean, how that would work and how other agencies deal with that? Do you understand what I'm saying?

Mr. HARTZOG. Sure. Sure. So it's difficult for me to speculate on the way that other agencies deal with that. But I will say that it's important to remember that when the FTC gets information about a potential breach or a vulnerability, that's just the very beginning of the inquiry, right? So the FTC doesn't police data breaches; the FTC polices unreasonable data-security practices.

Now, a breach can be evidence of a data-security practice, but that's just the starting point, right? So if you look at the complaints, the complaints actually have kind of a litany of data-security failures, so failure to have a training program and failure to implement administrative and technical and physical safeguards. And all of these things are things that are incumbent upon the FTC to actually prove if they allege them in the complaint.

And so I think that we want to be careful not to assume that just because the FTC has been notified of a breach, that that immediately means that the company that suffered the breach is liable, right? So the FTC is—it's on the FTC to fill that out, right, to say, well, what actually were the—were there unreasonable data-security practices that allowed this breach to happen? Or was this a breach that was going to happen regardless of whether there were reasonable data-security practices?

And that, to me, is really where the FTC, you know, starts doing its real investigative work, in that, you know, the notification of a breach is just kind of the first tip that leads to an investigation.

Chairman ISSA. Thank you.

Mr. Clay?

Mr. CLAY. Thank you, Mr. Chairman, and thank you for conducting this hearing.

Some critics of the FTC's approach to data protection have argued that the FTC has not provided adequate notice of the guidelines a company must follow to avoid an enforcement action. For example, in Federal litigation in New Jersey, Wyndham Hotels argued, "If the FTC can regulate data security at all, it must do so through published rules that give regulated parties fair notice of what the law requires."

Professor Hartzog, do you agree that published rules are required to give organizations notice of the data-security standards that are required?

Mr. HARTZOG. I don't think that that's necessarily accurate. I think that administrative agencies like the FTC actually have the choice of publishing rules or proceeding in a case-by-case basis and establishing the contours of the law in that way.

And, in this instance, when you have a complex and ever-evolving problem like data security, which is really more of a process than a set of rules, then the FTC has chosen, and I think probably wisely, to proceed in a case-by-case basis in order to incrementally establish rules and be adaptive to the ever-changing needs of consumers to have their data protected.

Mr. CLAY. Well, how can a company know when it's going to run afoul of the data-security requirements if they don't have notice of the rules?

Mr. HARTZOG. I would actually argue that they do have notice of what's required. So there are several different things that you can look to. When you have a reasonableness approach, the FTC isn't the only agency, the only regulatory scheme that uses a reasonableness approach. So States do, and there are other statutes that take advantage of it.

And you can look to basic things, right? So even in the statement that the FTC issued on its 50th data-security complaint let it know that there are really five basic things that you have to do. You

know, you have to identify your assets and risks; you have to minimize data; you have to implement safeguards; and you have to have a breach response plan. And those are the basic components.

And the way that you then fill that in is you look to lots of different variables, like the size of the company and the sensitivity of the data and the amount of data that you're collecting and the resources that you have available, which of course vary wildly according to company.

And so it actually, I think, would be a mistake to try to put those into rules because they inevitably would be either overinclusive or overprotective or underinclusive depending upon the context. And so, really, the only way forward, in my mind, is to proceed upon a reasonableness basis here.

Mr. CLAY. Okay.

Other critics of the FTC Section 5 enforcement authority have argued that the FTC should establish bright-line data-security standards in advance of any enforcement measures delineating exactly what companies must do to comply with this data-security obligation.

Professor Hartzog, in your recent article on the FTC and data protection, you address this point, writing, "Many critics want a checklist of data-security practices that will provide a safe harbor in all contexts. Yet data security changes too quickly and is far too dependent upon context to be reduced to a one-size-fits-all checklist."

Professor, can you elaborate briefly on what you mean here? How is data security changing in ways that make formal rulemaking impractical?

Mr. HARTZOG. Sure. So I've spoken with a lot of data-security professionals in doing my research, and they almost uniformly tell me that you can either have a one-size-fits-all checklist that lists the 17 things that you're supposed to do or you can have good data security, but you can't have both.

And the reason why that is is that data security changes so much, and it wouldn't make much sense to say that small businesses have to follow the same data-security protocols that Target and Amazon have to follow. And so it actually is very dependent upon all these variables.

And to the extent that we've heard testimony today saying that, you know, oh, well, we have guidance from HIPAA and we have guidance from Gramm-Leach-Bliley, I would ask everyone actually to look at the complaints filed by the FTC. They're very similar to the requirements in HIPAA and Gramm-Leach-Bliley. And so, to the extent that everyone is kind of fine with the way that those work, I think you can see similar kinds of requirements in the complaints filed by the FTC.

Mr. CLAY. And you also wrote that flexibility to adapt to new situations, the FTC can wait until a consensus around standards develops and then codify them as this happens.

Mr. HARTZOG. That's correct. So one of the problems with formal rulemaking is that if you make it too technologically specific, then by the time the rule actually gets passed, it's become outdated and you've got to start the whole process all over again, and it becomes

this never-ending series of trying to update standards that have become outdated.

We've actually seen this in other areas of the law where we've tried to list out technological specifications, and we now get routinely frustrated, you know, that they're outdated because it changes so quickly.

Mr. CLAY. Thank you for your responses.

Mr. Chairman, my time has expired.

Chairman ISSA. Thank you, Mr. Clay.

Well, we're going to come to a close, which is probably blessed for all of you. But I have just a final set of questions, and I'm going to go to each of you.

Mr. Hartzog, I hear everything you're saying, but if I'm to believe what you're saying, the complaints and the consent decrees are supposed to be my guidance as to what I have to do. I have to find within the complaints a company and a set of information that's similar to mine to figure out what I should or shouldn't do.

But even then, the consent decree says, we're going to keep an eye on you for 20 years. So, 2 years later, 3 years later, what they're doing behind closed doors in their oversight of that one company, I don't have visibility on that.

So how am I supposed to know what the law is?

Mr. HARTZOG. So I would actually say, instead of looking kind of to the consent decree, you look to the complaints. And the complaints actually point to industry standards, right? And there are various, actually, standards you could look to. So you could look to——

Chairman ISSA. But none of those standards are safe havens; is that right?

Mr. HARTZOG. Well, no, not explicit safe havens, but I think the understanding is——

Chairman ISSA. But wait a second. If I go 34 miles an hour in a 35-mile-an-hour zone, I'm not going to get a speeding ticket. Is that right?

Mr. HARTZOG. I'm really glad you brought that up. So Mr. Stegmaier brought up the whole speeding-limit thing, as far as how that's adequate notice. I would also add that if you look at speeding rules, in inclement rules the speeding rules actually change; they say drive reasonably under the circumstances. And yet we don't have a problem with that speeding law, which is, of course, based on a reasonableness standard.

Chairman ISSA. That happens to be an interesting law, because it only gets enforced when you have an accident, and then they will sue you. They will claim that you were driving too fast for conditions.

I appreciate the fact that you noted, then, that when the "fit hits the shan," when things go bad—I worked on that for a long time; I want you to appreciate that—then they will write you a ticket, when even when you drove the speed limit something happened. But there has to be a bad occurrence for that to be enforced. So I think we're all agreeing it's a good example.

But cybersecurity is a real question. I don't know everything about LabMD. I don't know everything about Open Door. But I will tell you that people right now, whether they have a server in a

closet and they're buying the latest software from Microsoft and other companies or they're up on Amazon or somebody else's virtual network, they don't know what the standard is.

I know one thing. Target and the U.S. Government at HealthCare.gov spent millions of dollars on security, hired countless experts in and out of house, and they were obviously data failures. So it's an inexact science.

The Federal Trade Commission has a mandate to protect us as consumers from, effectively, willful or reckless behavior. LimeWire participated in reckless behavior in the switches, how they had them turned down, what the default was, perhaps even on the peer-to-peer. But, certainly, because they made you most vulnerable, unless you knew a lot about the software and installation, they created a vulnerability which, quite frankly, was intentional.

And in a hearing before this committee, we pretty much got that, that they were—they thought it was great to open wide, when, in fact, they were implying it was small. To me, that's what the Federal Trade Commission was supposed to go after. They just weren't, apparently, an easy enough target.

So as we look at, not Section 5 authority—because I believe that Section 5 authority intended on deceptive and unfair practices in the Internet world, in the cyber world, being an authority; I think they did. But I think they wanted us to go after LimeWire, after people who claimed things.

And, quite frankly, I think maybe they want to go after a company like Tiversa, who goes around and trolls all over the Internet, using expertise that some might say was similar to the CIA—who, by the way, paid Tiversa at one point. And they go out and they find all these vulnerabilities, and then they turn them into business practices. And, in fact, every indication is they not only found the vulnerabilities but they stole information off those products. They stole them after the CEO of that company testified that these people were victims. Mr. Boback testified before this committee that people whose employees loaded LimeWire were victims, that, in fact, the person loading LimeWire was a victim because he or she didn't understand that they were creating the vulnerability.

So the very person who said you're a victim of this peer-to-peer software before this committee then used that vulnerability to pull data, to steal data. And to the extent they stole data only so they could inform the company and show them that it happened, I might say that it wasn't wrong. But to the extent that it was $475 an hour, that becomes a little more questionable. To the extent that they then go to the FTC if you don't say yes, as though they have a civic obligation.

Our discovery is not finished, but at this point it appears as though if you paid Tiversa, you never would've gotten that letter from the FTC. Mr. Daugherty, if you'd paid Tiversa, you never would've had these years of agony. And for just a few hundred thousand dollars, you probably would still have a going concern instead of litigation ongoing.

Now, that doesn't go to the merit of the letter, it doesn't go to the merit of the suit. It goes to the whole question of the practice. We haven't passed a law that says, if you go out and surf the Internet, look for vulnerabilities and take things off of people's private

sites, including HIPAA-related material, that, in fact, you're a criminal. Maybe we should. And that's within the jurisdiction of Energy and Commerce and other committees, and we take it seriously. And it's one of the reasons that this hearing is important.

Now, I have a closing very self-serving question, mostly for, if you will, my two company victims. Things have been said here and allegations made and questions about Tiversa as a company. I don't normally investigate companies. It's not the practice of this committee.

But given—and I'm going to leave Mr. Daugherty, because you're in a lawsuit. I'm just going to leave you out of it for a moment.

But, Mr. Roesler, your case is completely finished; is that correct?

Mr. ROESLER. It is.

Chairman ISSA. And so you're done, you have no financial interest in anything that we look into; isn't that correct?

Mr. ROESLER. That's correct.

Chairman ISSA. So do you believe it's reasonable for this committee to find out what Tiversa took off of your Web site or your site or some other site, where they got that information that they approached you with an offer to sell you services?

Mr. ROESLER. I believe it's worth the while if there's a pattern, that I am not the only victim, then it's worth the while.

Chairman ISSA. If we thought you were the only one, we wouldn't be here.

Do you believe it's important for us to verify the relationship between Tiversa and the various companies—many of whom we have lists of, so we know you're not the only one—that they turned over to the FTC based on one question? The ones that they offered services to that bought the services where they never turned over to the FTC, but ones who declined were often turned over to the FTC. Is that a question you think we should find out the answer to?

Mr. ROESLER. I believe that would be a very good question.

Chairman ISSA. And, lastly, the law firm that sued you in a class action, do you believe it's fair for us to find out whether there was a direct connection between these two Pittsburgh-based companies and data taken from somewhere yet unknown, provided to the law firm, and the law firm then going out and reaching out to your patients and clients? Do you believe we should ask those questions as part of a broader investigation to find out whether, in fact, that was coincidence or, in fact, an attack on your company because you didn't buy their services?

Mr. ROESLER. Mr. Chairman, one of the reasons why I'm glad to be here today is the hope that possibly that question could be answered.

Chairman ISSA. Well, I'm going to recognize Mr. Cummings.

These are some of the areas in which I believe that somebody should investigate. For now, the somebody is us. Our hope is that the FTC IG, who has some authority but not as much as we do, oddly enough, to get information from nongovernment entities, and perhaps the Justice Department and others will look into it.

But until we find somebody else, at least for the foreseeable future, my intent is to continue asking those questions. We will invite Tiversa and others in. As I said at the opening, I would hope

to hear—that all the Members would hear from the whistleblower, not because his accusations are alone of anything other than the basis under which we began this, but because when you get one set of allegations and you go out to corroborate them and you have those as a first statement, then when you find the second corroboration, normally it allows you to show that it is true. I want to get to the truth. I know Mr. Cummings does.

So for all of you, Section 5 authority—it's not our job to second-guess what Congress gave them. They gave them the authority. Section 5 authority, it is for us to ask, are they acting in a way that allows unfair actors to be held accountable and others to know how to meet their obligation? You have our commitment, we intend to continue and do it.

As to unfair practices practiced in the cyber world and as to people's vulnerabilities and how they correct it, this is an ongoing part of this investigation. The questions I asked you, I said they were self-serving. It's the intent of this committee to continue for as long as it takes to feel that all parties are satisfied that we asked all the right questions and got as many answers as we could.

Mr. Cummings?

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

When I—first of all, I want to thank the witnesses for being here. You know, sometimes I think witnesses wonder whether they have an impact. And I can tell you that all of you were excellent. And I really appreciate what you said, and I think the Members listened to you very carefully.

When I first read the title of the hearing, I was very concerned with the question of whether FTC has the authority to pursue data-security enforcement actions under its current Section 5 authority. And I think, based upon what the chairman just said, I think we all agree that they do. And I agree with him, the question is how they go about doing that.

And I think that there are moments that present themselves in our lives where we have to stop for a moment and at least take a look at what we're doing and how we're doing it.

Mr. Roesler, Mr. Daugherty, as I said before, if you've been treated unfairly—you know, and both of you are dealing—your businesses dealt with health issues, right? Health. And health is a big, big deal for me, personally, and I'm sure it's a big deal for most of us. But I want us to be very careful.

You know, government does have a role to play. It really does. When people's information is out there, their lives can be turned upside down. I've had people come to me as a Congressman, talk about their identity being stolen and taking years and years to get it back. We have to have some folks making sure that we protect as best we can against that.

And I think that there's always a balance. You know, there's got to be a balance so that we don't just run over people like you, Mr. Roesler, and you, Mr. Daugherty, but, at the same time, make sure that folks who are aiming to do these kinds of things know that we're not going to stand for it and that somebody's going to be looking and somebody's going to bring them to justice.

So that's where, you know—that's—you know, if you listen to everything that has been said here today, I think that's what it pretty much boils down to. How do we strike that balance?

And so I thank you, Mr. Chairman. I think it was a good hearing. I look forward to hearing from the FTC. And you're right, trying to hear from the FTC is going to be kind of tricky, because it seems as if—I mean, if you could limit the questions to their general procedures without getting into the case, I think that might be helpful, but it's going to be tricky. But I think we do need to hear from them as to how they go about this.

But, again, this is a critical moment. And I think we need to try to take advantage of it so that, if something needs to be corrected, that we correct it. I think anybody wants to have some idea of what they're being accused of. I mean, was there ways to get the information out in a better way? You know, this is what you need to look out for. It's just like when you're riding down the road and it says, you know, 25 miles an hour, radar enforced by photos. You know, I mean, at some point, it's nice to have a little notice. And all of us know after we've gotten a ticket or two that we slow down. And we know those areas by heart; we just know them.

And so, again, I thank you all for your testimony. I really, really appreciate it.

And thank you.

Chairman ISSA. Thank you.

I'll leave the record open for 7 days, not only for Members to put in opening statements and extraneous material, but for the witnesses to provide any additional information they deem appropriate as a result of the questions here.

Chairman ISSA. I want to thank you for your testimony. I want to thank you for making this a worthwhile hearing.

And we stand adjourned.

[Whereupon, at 12:24 p.m., the committee was adjourned.]

○