S. HRG. 111–601

# VIDEO LAPTOP SURVEILLANCE: DOES TITLE III NEED TO BE UPDATED?

## HEARING

BEFORE THE

## COMMITTEE ON THE JUDICIARY
## UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

MARCH 29, 2010

PHILADELPHIA, PENNSYLVANIA

**Serial No. J–111–83**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

58–268 PDF WASHINGTON : 2010

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 THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
EDWARD E. KAUFMAN, Delaware
ARLEN SPECTER, Pennsylvania
AL FRANKEN, Minnesota

JEFF SESSIONS, Alabama
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MATT MINER, *Republican Chief Counsel*

# CONTENTS

## STATEMENTS OF COMMITTEE MEMBERS



## WITNESSES



## SUBMISSIONS FOR THE RECORD

# VIDEO LAPTOP SURVEILLANCE: DOES TITLE III NEED TO BE UPDATED?

**MONDAY, MARCH 29, 2010**

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
*Washington, DC*

The Committee met, pursuant to notice, at 10:00 a.m., U.S. District Court for the Eastern District of Pennsylvania (Philadelphia), Courtroom 3B, Hon. Arlen Specter presiding.

## OPENING STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Chairman SPECTER. Good morning ladies and gentlemen. The hour of 10:00 having arrived, the Judiciary Subcommittee on Crime & Drugs of the Senate Judiciary Committee will now proceed with this hearing which has been entitled Video Laptop Surveillance: Does Title III Need to Be Updated?

There was a recent incident at Lower Marion Township High School where video laptops were taken from the school into private residences and on one of these laptops it was activated so that the surveillance can be conducted secretly or there could be seen what was going on inside of private homes which raises an issue of violation of privacy.

Privacy is one of our most prized values in our society protected by the Fourth Amendment of the Constitution of the United States and by a variety of federal statutes. The incident raises a question as to whether the law has kept up with technology or there to have been an interception of a telephone communication it would violate federal law or there have been a secret surveillance with sounds that would have been a violation of federal law, but there appears to be a gap where there was no sound but only an opportunity to watch what people were doing inside a private residence.

Our inquiry here is not directed to this specific incident or incidents or whether the school district acted properly or whether there was any civil claim. There is litigation pending in the federal court on that subject, but the inquiry of the subcommittee is focused on the public policy question as to whether federal law ought to be changed.

We have a very distinguished array of expert witnesses who have traveled here from far and wide to give us their views on this subject.

Professor Frederick H. Cate from the Indiana University School of Law in Bloomington and Director of the Indiana University Center for Applied Cybersecurity will be our lead witness.

We will have testimony from Mr. Marc Zwillinger, founding partner of Zwillinger Genetski, a law firm specializing in the complex laws governing internet practices.

Mr. Kevin Bankston, Staff Attorney specializing in free speech and privacy law with the Electronic Frontier Foundation.

Mr. Richardson, Mr. Robert Richardson, Director of Computer Security Institute specializing in security trends and strategies for protecting information.

Mr. Jack Livingston, Chairman and CEO of Vancouver based Absolute Software Corporation.

We have a lot which is happening on the Internet and we have a great deal which is happening in cyberspace, real issues as to national security and related fields, a real issue to commercial enterprises being able to protect their trade secrets.

Looking back at one of the landmark decisions at American Jurisprudence, Olmstead versus the United States Justice Brandeis made a comment about a violation of Fourth Amendment rights of the defendant stating that, "In the application of a constitution, our contemplation cannot be only of what has been but of what may be."

Justice Brandeis was prescient in so many ways and he was here looking at a complex issue decades removed. When you talk about the right of privacy, we live in a complex society. We have been battling in Washington the issue of warrantless wire taps, the power of the President under Article II as Commander in Chief contrasted with the authority of Congress under Article I on the Foreign Intelligence Surveillance Act in cyberspace and the Internet, a very prized American valued privacy is at issue here. We are going to try to find out where we ought to head.

We turn now to our first witness, Professor Cate whom I have already introduced in effect. Professor Cate, the floor is yours.

**STATEMENT OF FRED H. CATE, PROFESSOR OF LAW AND DIRECTOR, CENTER FOR APPLIED CYBERSECURITY RESEARCH, INDIANA UNIVERSITY MAURER SCHOOL OF LAW, BLOOMINGTON, INDIANA**

Mr. CATE. Thank you very much, Mr. Chairman, and let me say how much I appreciate both your holding this hearing on this very important subject and your including me in it. It is a privilege to also be on such a distinguished panel of other commentators on this issue.

I have just three points which I will make quite briefly. The first is there is no question but that Title III of the Omnibus Crime Control and Safe Streets Act, what we refer to as the Wire Tap Act, needs to be revised. It does not cover video, unaccompanied surveillance video unaccompanied by sound, and therefore in situations such as that which has given rise to this hearing, those situations are not covered by the Wire Tap Act.

The reality that the Wire Tap Act does not extend to video or other optical surveillance if the sounds are not captured at the same time has been highlighted in many prior situations in which cameras were installed in bedrooms and bathrooms and changing rooms and elsewhere causing some states to enact video voyeurism laws.

To avoid this gap in the future, it is going to be necessary to either amend the Wire Tap Act or to enact some other standalone piece of legislation. But doing so is not going to be quite as simple as it may sound because the Wire Tap Act deals with intercepting communications between parties and not the mere observation of parties or the observation of a setting such as a bedroom. Therefore, it will also be critical not to make any amendment to the Wire Tap Act so broad that it restricts the use of security cameras in public, which serve a very important purpose and one that I don't think anyone would wish to eliminate.

So it is clear that the gap needs to be closed. It is less clear precisely as to how that will be done, but it is certainly Congress who will have to do it.

The second point I would like to make is that the alleged use of the laptop camera to capture images of a student within his home is only the most recent in a long series of events that we have seen in which modern digital technologies are deployed in ways that challenge both existing laws and our existing understanding of privacy.

So RFID tags, GPS devices, cell phones and cell phone cameras, OnStar and other vehicle assistance services, digital audio and video surveillance technologies that have exploded in cities largely thanks to federal funding and other technologies are constantly challenging our understanding of what is and what should be private.

So individual courts are grappling with these issues and states are grappling with these issues, but increasingly it is clear that it is the thoughtful intervention of Congress that is necessary to resolve this conundrum.

In 2004, the Technology and Privacy Advisory Committee which was appointed as an independent committee to oversee the situation created by the Terrorism Information Awareness Program and the Department of Defense concluded in its final report current laws are often inadequate to address the new and difficult challenges presented by dramatic developments and information technologies and that inadequacy will only become more acute as the storage of digital data and the ability to search it continue to expand dramatically in the future.

That panel recommended, and I quote, "It is time to update the law to respond to new challenges." Now, that was 2004. I think later this week we will be hearing from a large coalition led by the Center for Democracy and Technology that has been working for almost two years to develop specific principles around which revision of these laws might be based.

I know that the members of that coalition are eager to work with you and with members of this Subcommittee and the Judiciary Committee to develop an appropriate and balanced update to the law.

The final point that I would like to make is that there are important steps that institutional providers, users of these digital technologies can and should already be taking irrespective of their specific legal obligations to diminish the impact of those technologies on privacy and other protected civil liberties.

For example, having in place written policies on the use and the retention of the material, having in place oversight mechanisms, audit tools, designated chief privacy officer or chief compliance officer to ensure that those rules are being followed, and in many ways perhaps most importantly, a level of transparency so that any users of those technologies know what they should reasonably expect when using them.

Now, I don't want to belabor those in this testimony, but I think those are important not only for individual users to be concerned with, but may also play an important role in whatever form of legislative recommendation you and your colleagues craft so that we see not merely a binary black and white on or off—either it is private or it's not private—but rather we see in place tools to help maximize privacy even while engaging in surveillance that may be necessary or serve very important values.

So my time is up. Let me say again how much I appreciate your having launched this very important dialogue. Thank you, sir.

Chairman SPECTER. Thank you very much, Professor Cate. Our next witness is Mr. Mark Zwillinger, founding partner of Zwillinger Genetski, a law firm specializing in the increasing complex issues governing internet practices including wire taps, Communication Act, privacy and spyware.

Thank you for coming, Mr. Zwillinger and we look forward to your testimony.

**STATEMENT OF MARC ZWILLINGER, PARTNER, ZWILLINGER GENETSKI, L.L.P., WASHINGTON, DC**

Mr. ZWILLINGER. Thank you, Chairman Specter. I'm pleased to appear today to discuss the topic of amending Title III to include video surveillance. My views on this issue come from my prior experience as a federal prosecutor, my current work in private practice in privacy and security issues and my role as an adjunct law professor at Georgetown University Law Center.

Every so often we become aware of an incident like what happened in Lower Marion that makes us question whether our privacy laws are adequate. This past fall, similar concerns came up when a man tracked ESPN reporter Erin Andrews around the country, installing secret cameras in her hotel rooms and capturing and uploading videos of her to the internet.

A review of recent cases demonstrates other abuses of surveillance technology to film people in places where they should expect privacy, including landlords who have secretly videotaped tenants, hotel managers who have spied on guests, and schools who have videotaped students in changing rooms.

Title III does not address these problems because silent video surveillance is not covered by the statute. But while it's tempting to conclude that Title III should prohibit this behavior, amending it to do so would likely be a mistake.

Just as we are troubled that our remote video surveillance of children can be possible in private places, we rely on secret video surveillance to keep us safe—from the cameras that protect our children at places like Hershey Park or Sesame Place to the closed circuit TV cameras outside our apartments. Silent video has become our extra set of eyes.

Companies regularly use technology such as silent video to protect their employees and their property. Therefore, when we consider how to prevent abuses of our surveillance, we must not ban the uses of technology that does strike the right balance between privacy and security.

Now, as written, Title III serves three distinct purposes. It places limits on law enforcement, it defines what is a federal crime and it creates a civil cause of action. But it only does so with respect to wire communications like phone calls, electronic communications like emails and oral communications, like the things we say to each other in person.

Now, wire and electronic communications are covered in all circumstances, but oral communications are only covered where the speaker has a reasonable expectation that their communication will be private.

Clearly we cannot equate videos and photos to wire and electronic communications under Title III. This would make thousands of security cameras in public places illegal and it would turn parents and journalists and security professionals into criminals. Therefore, video surveillance like oral surveillance and oral communications would have to be prohibited only where the person has a reasonable expectation of privacy.

Even then, adding video to the Title III framework may create more problems than it would solve. As to the government, the Courts of Appeal have already held that video surveillance in a private area must comport with the Fourth Amendment and that search warrants for video surveillance must meet existing Title III standards.

So when it's the government that's peering into citizen's homes, the constitution may already provide an effective remedy. But adding video to Title III would create tremendous problems for the private sector.

Under Title III, the standard for when oral communications may be recorded without consent is the same fact-based reasonable expectation of privacy test under the Fourth Amendment. So predicting in advance when it is acceptable to record audio under this standard is difficult. That judicial opinions teach us that the answer is frequently "it depends". It depends on the location, it depends who is captured, what they were doing, whether third parties would be anticipated to be present, whether you needed technology to do the oral surveillance, and more.

If you apply this body of existing case law to video surveillance, it would raise very hard questions, especially in those semi-secluded places where we do want video cameras, like in elevators with no other passengers or in the locked entrances of banks where ATMs may be located.

If Title III included video, every wrongdoer who was caught on a security camera in these areas would challenge the lawfulness of the surveillance. Evidence of crime in private secluded spaces could be suppressed, companies could be held liable and none would want to be on the hook for installing cameras due to the risk of civil liability or criminal punishment. This is one of the reasons why video surveillance is silent today. The risk of capturing audio is too great.

Instead of Title III, there are more targeted alternatives that could address the privacy concerns raised by the Lower Marion and Erin Andrews examples without diminishing our security.

Generally video seems to concern us most when it intrudes in the home or an area where someone may be naked, when legitimate surveillance tools are redirected for voyeurism and when it involves children.

Legislation to prevent these first types of intrusions on federal land was already enacted in the Video Voyeurism Prevention Act of 2004 which prohibits voyeurism in areas where people could reasonably be expected to change clothes without prohibiting the legitimate use of surveillance in quasi-public places.

This approach is not perfect. It doesn't cover all of the examples where we wouldn't want video surveillance, but it provides a better starting point than Title III for a comprehensive federal statute that protects private spaces from video intrusion.

Several other states have also tried to take on this problem. Some examples are cited in my written testimony. Delaware, for example, focuses on the place where the surveillance is installed and whether people have a reasonable expectation of privacy in that place.

These state laws, like the Video Voyeurism Prevention Act could serve as a model for future federal legislation. Such legislation could also have a safe harbor from liability for organizations that use security cameras if they have adequate controls to prevent against rogue uses of the technology.

In conclusion, the idea that our children can be subject to video surveillance in private areas is troubling. But what really bothers us about video surveillance is the fact that the camera may catch us unaware or even undressed.

In the hierarchy of privacy protection, we should be more focused on ensuring that our private thoughts, our conversations, our phone calls, our emails and our instant messages remain private and that neither the government nor private individuals can get access to them without adequate notice or probable cause to believe that we are committing a crime.

There is no question that our privacy statutes are in need of reform, especially to bring the privacy protections for electronic communications into the modern age of computing. But when we are addressing video surveillance, we need to carefully craft legislation to target the specific harms we're going after without eliminating the ability to use silent video for security purposes.

Thank you for the opportunity to testify. I look forward to answering your questions and working with the subcommittee.

Chairman SPECTER. Thank you, Mr. Zwillinger. Our next witness is Mr. Kevin Bankston, Senior Staff Attorney specializing in free speech and privacy laws with the Electronic Frontier Foundation.

He has worked, he has focused on the impact of post 9/11 antiterrorism laws and surveillance initiatives on online privacy and free expression.

We appreciate your coming in, Mr. Bankston and appreciate your testimony.

**STATEMENT OF KEVIN BANKSTON, SENIOR STAFF ATTORNEY, ELECTRONIC FRONTIER FOUNDATION, SAN FRANCISCO, CALIFORNIA**

Mr. BANKSTON. Thank you. Senator. Thank you. Good morning, Chairman Specter, and thank you for inviting me to testify here on behalf of the Electronic Frontier Foundation on this very important subject.

Laptop cameras or webcams represent an awesomely useful new technology. However, this new technology also carries with it an awesome new privacy risk with millions upon millions of laptops being carried with webcams routinely being carried into the home and other private spaces.

Surreptitious video surveillance has become a newly pervasive threat. Put simply, any camera controlled by software on a computer that is connected to the internet carries the risk that the camera will be remotely activated without the knowledge of the user, whether by stalkers, computer criminals or even foreign governments using malware or malicious software to break into the computer and take control of the camera or by schools or employers with the ability to install their own software on their computer or by U.S. state or local government law enforcement investigators attempting to monitor a suspect.

Recent allegations that school administrators of the Lower Merion school district have secretly photographed students inside their homes using the webcams on student's school-issued laptops have put a spotlight on how this new technology puts American's privacy at risk and should be a wake up call to Congress to address a troubling gap in privacy law.

As the other commentators have noted, Title III, otherwise known simply as the Wire Tap Act currently only regulates electronic eavesdropping on private conversations and the wire tapping of voice and electronic communications or in terms of the statute, it only regulates the interception of oral, wire or electronic communications.

It does not regulate the unconsented video surveillance of private spaces as the legislative history makes clear and as all seven federal circuit courts to consider the question have held.

So, for example, secret monitoring of your email transmissions, wiretapping of your telephone calls or secret eavesdropping using a microphone hidden in your home, all of these would violate Title III. However, the secret use of the webcam or a radio controlled camera to photograph you inside your home would not violate Title III because in such a case there would be no oral, wire or electronic communication of yours to be intercepted.

Even though such secret surveillance can be as invasive if not more invasive than listening in on your conversations or monitoring your internet communications, Title III simply doesn't apply.

Judge Posner of the 7th Circuit who in 1984 in the Case of *U.S.* v. *Perez* wrote the first Circuit Court opinion applying this logic holding that Title III does not regulate video observed in that opinion of course it is anomalous to have detailed statutory regulation of bugging and wiretapping but not of television surveillance in Title III.

We would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope.

Over 25 years have passed since Judge Posner first recommended such a change, but Congress has not yet acted even though the threat of surreptitious video surveillance has increased exponentially along with the number of internet connected cameras.

We at EFF are therefore thankful to this subcommittee for taking up the issue and reexamining the question of whether Title III should be updated to regulate video surveillance because, to put it bluntly, the current inapplicability to Title III doesn't make sense.

It makes no sense that if the school administrators had eavesdropped on student conversations at home using the laptop's microphone or it intercepted a student's private video chats they would have clearly violated Title III, but equally invasive video spying is not regulated by the statute at all.

It also makes no sense that a public school or any other governmental entity that wanted to legally spy on a student in this matter would have to get a prosecutor to obtain a probable cause warrant that satisfies Title III's core requirements in order to comply with the Fourth Amendment, yet a private school could do so without any regard to Title III at all.

Finally it makes no sense that Congress while strictly regulating electronic eavesdropping would leave the regulation of equally invasive video surveillance up to the states. As in 2003 when the Reporters Committee for Freedom of the Press last surveyed the state of the law, only 13 states had passed statutes expressly prohibiting the unauthorized installation or use of cameras in private places, and several of those statutes regulate cameras only in certain limited circumstances such as in locker rooms or restrooms or where the purpose is to view someone who is partially or fully nude.

One federal law mentioned by Mr. Zwillinger, the Video Voyeurism Prevention Act of 2004, similarly restricts only secret videotaping persons in a state of undress and only applies in the special maritime and territorial jurisdiction of the U.S. rather than applying generally.

It is EFF's opinion that in the face of the 21st Century landscape literally littered with cameras that are vulnerable to abuse, this kind of patchwork response to a growing nationwide problem is increasingly unacceptable.

In conclusion, Mr. Chairman, the Committee asked us whether Title III needs to be updated in light of video laptop spying and EFF's answer is plainly yes. Title III should cover video surveillance in private spaces where there is a reasonable expectation that you won't be photographed.

We look forward to the possibility of working with the subcommittee to update the law to regulate video surveillance in a manner that appropriately balances the interest of privacy and free expression and public safety, but would also echo the comments of Professor Cate and Mr. Zwillinger that this is only one area where our electronic privacy statutes need to be updated. We look forward

to an announcement hopefully this week of this coalition's work which we are also a part of.

In the meantime, thank you again for having us and I look forward to your questions.

Chairman SPECTER. Thank you, Mr. Bankston. Our next witness is Mr. Robert Richardson, Director of Computer Security Institute, a professional membership organization for information security professionals.

That institute seeks to follow security trends and recommend strategies for organizations seeking to protect their information and technology.

Mr. Richardson, we appreciate your coming in. The floor is yours.

**STATEMENT OF ROBERT RICHARDSON, DIRECTOR, COMPUTER SECURITY INSTITUTE (CSI), SWARTHMORE, PENNSYLVANIA**

Mr. RICHARDSON. Chairman Specter, thank you for inviting my written statement and for this opportunity to speak to the issue of video surveillance, particularly as it relates to surveillance using common consumer mobile computing devices such as notebooks, cell phones and personal digital assistants.

These devices, because of their ubiquity, clearly present opportunities for enhanced communication, but they also challenge our notion of security practices as they relate to privacy and surveillance.

As Director of the Computer Security Institute, I am engaged daily with these issues as they relate to organizations that maintain large computer and network infrastructures.

The instigation for our discussion today was the desire of one such organization to protect its computer assets, and as one would probably expect, concern that mobile assets may be lost or stolen is completely well-founded.

One project undertaken by the Computer Security Institute over the past 14 years is an annual survey of our information security professional community specifically within the United States. In the most recent survey, 42 percent of 443 respondents said that their organizations had suffered the theft of laptops or mobile devices in the previous year. Only infection by malicious software or malware reported by 64 percent of the respondents was more prevalent.

Perhaps ironically the modus operandi of today's sophisticated malware is not at all unlike that of the software deployed by some organizations to monitor their notebook computer assets. Both with tracking software and malware, this fundamental level of direct control of the device is transferred to a third party at a distance.

This transfer is achieved in both cases because malware and tracking software have gained or been granted access to the most extensive level of control of the computer, so called root control.

Most issues of privacy and access within the confines of a computer have at their root the issue of root access.

When the owner and primary user of a device are one in the same, control and responsibility is easily understood and it is the user who has control of the root account. But in the instance of say an employer that loans a notebook to an employee, the employer may well withhold root privileges from the employee. This gives the

employer more control over the device than the user and indeed more control than the user may be aware of such as the ability to remotely operate a built in camera.

Root control may be abused in many ways, including by surreptitious spying. But this notion of root control is a necessary one and extended only slightly gives us an opening to separate and protect different categories of use within a device. There can be a category of work place use, for example, that is entirely walled off from personal use.

There are multiple ways to achieve this that would be too lengthy and technical a discussion to delve into here, but in fact most Americans are already familiar with one such division of control. Ninety five percent of cell phones sold each year within the U.S. are locked phones meaning that their use is controlled and restricted by the carrier that originally sold the phone and that is providing service to it.

Using the phone for conversation or texting is understood to be a context where the user is in control. That same user, however, cannot update the core software that runs the phone. The service provider can and does because the service provider has what is in effect root control over the phone.

It is possible in short to lock down part of a system so that the locked down element's function has a complete computer system under themselves with separate software applications and separate storage for files. That this lock down environment is truly separate from the rest of the computer can be rigorously demonstrated using well understood techniques based on advanced forms of encryption as well as a computing framework known as trusted computing.

Almost all notebook computers sold since 2004 include a trusted platform module housed in a sealed, tamper proof component within the computer. This provides a reliable foundation for protected, high control partition of the computer.

In the vast majority of cases, however, this TPM functionality is not enabled and it would be disingenuous not to note that trusted computer systems have raised a great deal of controversy within the information security community.

This controversy, however, stems precisely from a fear that third parties, parties such as Microsoft, will have overreaching control over consumer owned PCs. This is not a concern when we are speaking of an organizational owner extending control over its own PCs. Within this lock down system of third parties such as a school or employer, they have an oasis of control. If they don't want to allow chat programs, chat programs can be barred. If they don't want pornography stored, they can scan for it and monitor employee use at will. The user of that system will know that whenever they are using the system in this workplace context, they may well be monitored.

On the same system, however, it is possible to use what is effectively a second computer that is not locked down or that is locked down in a less restrictive way.

That we can create clear technical boundaries means that we can by extension create clear legal boundaries. We have the option to legislate in a way that recognizes the possibility of such boundaries. By doing so, we can establish that the context in which any

kind of surveillance occurs is either clearly within or outside legal bounds.

Once again, I appreciate the opportunity to discuss this important issue and I will be happy to answer any questions.

Chairman SPECTER. Thank you, Mr. Richardson. Our final witness is Mr. John Livingston, Chairman and CEO of Vancouver based Absolute Software Corporation, a publicly traded global company specializing in tracking, managing and protecting computers and mobile devices and providing theft recovery. We welcome you, Mr. Livingston, and look forward to your testimony.

**STATEMENT OF JOHN LIVINGSTON, CHAIRMAN AND CEO ABSOLUTE SOFTWARE CORPORATION, VANCOUVER, BC, CANADA**

Mr. LIVINGSTON. Chairman Specter, members of the subcommittee, Absolute Software is pleased to have this opportunity to discuss Absolute's products and services as well as our protocols and policies as they relate to property protection and privacy issues which is something that Absolute values and cares deeply about.

I co-founded Absolute Software in 1994 with the notion that individuals and businesses should be able to manage, secure and recover the mobile devices, regardless of their physical location.

Since that time, Absolute has developed one of the premiere managed theft recovery services in the world. Our security as a service solutions protect more than 5 million computers worldwide for subscribers who range from individuals to large public and private sector organizations.

To date, we have recovered over 13,500 stolen computers in 50 different countries with our flagship service, Computrace. We average approximately 100 stolen computer recoveries each week.

Absolute believes very strongly in protecting Computer theft victims and mitigating the multiple downstream consequences of computer theft. For an organization with a stolen computer, the cost of hardware is really just the beginning. In addition to the lost productivity and competitive threats an organization experiences, an organization that experiences a data breech may be subject to fines, media scrutiny and a damaged reputation.

Computer theft has other costs and consequences, including the potential theft of personal identifying information that may later be sold or otherwise misused by identity thieves.

In fact, we have assisted the Philadelphia police on many occasions. We have an inspector and detective with us today, including cases where recovering laptop led to apprehending a child pornographer or recovering illegal drugs, weapons and stolen cash. This is not atypical.

Our case experience indicates that laptop thieves are often involved with other very serious crimes, including child pornography, identity theft, drug trafficking, home invasions, and of course large scale burglaries that may involve public school districts.

I will share a few brief examples. In San Diego, Computrace assisted a school district in recovering 13 laptops that had been stolen during a burglary. The thieves were also charged with possession of methamphetamines and various parole violations. In Chicago, Computrace uncovered an airline's luggage handler theft ring

at O'Hare Airport after which law enforcement arrested five workers and recovered eight laptops, four cameras, two GPS units and cash.

In Florida, Computrace helped to capture a career criminal who had been burglarizing offices nationwide and taking up to 12 to 15 laptops at a time. He was sentenced to 10 years in prison for his various crimes.

We believe our numerous successes are possible because our post-theft recovery services are carried out by Absolute trained theft recovery personnel. The theft recovery process only begins when the customer reports their computer as stolen to local law enforcement. Then the customer must report the theft to Absolute, provide the police theft report file number which is required before any theft recovery process begins, and give their authorization to have Absolute's theft recovery team start the investigation.

Our trained Computrace investigative team of law enforcement veterans coordinate the computer theft recovery process and cooperates with local law enforcement to recover the stolen property and return it to its rightful owner.

We are ISO 27001 certified and have policies, procedures and controls in place to protect customer data which I would be happy to describe if that has interest to your committee.

Thus, our Computrace solution is premised upon a managed theft recovery model that relies upon a filed police theft report to open a case investigation which is then handled by our staff of highly trained formal law enforcement personnel.

Some of our competitors instead offer end user solutions which operate in a manner similar to the Lan Rev Theft Track tool set where a purchaser such as an IT administrator at a school district could choose to enable taking still images from a laptop's Web cam.

Absolute did not itself offer Web cam functionality in its Computrace product line because we did not see a need for such a tool set in our very different and in our view, superior managed theft recovery model.

We acquired Lan Rev's assets late last year for their computer, inventory power management and asset management functionality. Through a software patch offered to the theft track customers we acquired, we removed the Web cam feature earlier this year.

With that, I conclude my comments. Thank you, Senator, for inviting me. I appreciate it very much and welcome your questions.

Chairman SPECTER. Thank you, Mr. Livingston. Well, it is a very intriguing, complex subject matter. I note the invitation from Judge Posner of the Seventh Circuit, a very distinguished federal judge in 1984 as the testimony has noted in inviting Congress to deal with this gap in federal law, and I note Professor Cate's comment that there is room for a "thoughtful intervention of Congress."

That may limit Congress' role. It is not so funny considering the legislation we passed last week and the public disagreement with it, although our job is to call them as we see them. In a representative democracy we have to make the judgments, to consider our constituents, but ultimately to make the judgments ourselves, we don't run by polling or public opinion polls.

That raises a threshold question which I ask of each of you. Does the passage of 25 years since Judge Posner's invitation for Con-

gress to fill the gap suggest that perhaps Congress ought not to act? What do you think, Mr. Livingston?

Mr. LIVINGSTON. We believe the current legislation that is in place, Senator, really does cover this well.

Chairman SPECTER. Which legislation in place do you think covers it well?

Mr. LIVINGSTON. Well, the different federal legislation and state legislation that's in place regarding how evidence might be gathered.

Chairman SPECTER. But there is no federal legislation which covers pure visual surveillance, is there?

Mr. LIVINGSTON. Senator, in our managed theft recovery model where we are representing the owner of the device, it is not a common carrier type situation.

We are actually able to locate a device with the owner's permission in cooperation with law enforcement. We feel that the existing law and the legal framework that's in place allows owners of computers and private property to be able to get their stolen computers back.

Chairman SPECTER. Well, that is where the issue is one of ownership and retrieval. But suppose that is not an issue. Suppose it is only a gap. The wire tap law says you can't have the interception of a telephone call, you can't have surreptitious surveillance, a secret surveillance if there is an oral communication but it leaves open if it is just visual.

So if you don't have retrieval of property, isn't the gap present?

Mr. LIVINGSTON. Sir, my only experience is representing the owner, the legitimate owner of the device in the context of it being lost or stolen. In that context, we have our internal processes and procedures in place to be able to effect a stolen computer recovery with the help of law enforcement. We work in that framework and that's all I can really comment on.

Chairman SPECTER. All right. That's fair enough within the purview of your experience, but there is a vast issue beyond your own particular purview.

While we are, well, let me move to Mr. Richardson. Do you think that the unanswered invitation, Judge Posner's unanswered invitation for 25 years suggests that Congress ought to stay out of it?

Mr. RICHARDSON. No, Senator, I don't. I think that two relevant changes that have occurred in the past 25 years that I would point to are the vast increase in Internet connectivity and specifically in high bandwidth Internet connectivity which makes the transmission of video images easily accomplished across the Internet in a way that was not possible when Judge Posner made those remarks.

Additionally, I think the ubiquity of camera devices embedded in mobile consumer goods is something that while it may be a difference in degree, it is an extraordinarily large degree of difference. I think basically there were no cell phones 25 years ago with cameras and my suspicion is that every cell phone in the room today has a camera, although I might be wrong.

But I think those two differences are, they really create an atmosphere that is ripe for abuse.

Chairman SPECTER. Mr. Bankston, what do you think? Should the federal government stay out?

Mr. BANKSTON. No, Senator. First I agree with Mr. Richardson that even if there were a good reason for Congress not to intervene in this issue in the past, the changed technological landscape really requires action here.

But I don't think that Congress made a reasoned decision to stay out of this in that it had an opportunity in 1986 with the Electronic Communications Privacy Act to make these updates. It clearly did not based on the legislative history which explicitly says this doesn't cover video surveillance.

Even though they noted Judge Posner's decision and other decisions applying Title III's requirements to video surveillance by law enforcement if only to satisfy the Fourth Amendment.

I have not been able to find any explanation for why Congress refrained from regulating video surveillance in 1986.

Chairman SPECTER. You have not found any explanation for why Congress refrained from doing something?

Mr. BANKSTON. No.

Chairman SPECTER. Have you on any other occasion? I have been there awhile and I haven't figured that one out myself.

Mr. BANKSTON. But I have my suspicions, Senator, and I think it was simply a drafting difficulty. As in particular Mr. Zwillinger pointed out——

Chairman SPECTER. Drafting difficulty?

Mr. BANKSTON. Well, a structural difficulty.

Chairman SPECTER. Weren't you available to help?

Mr. BANKSTON. I guess I was in high school back then.

Chairman SPECTER. Weren't you available to help?

Mr. BANKSTON. I am now available to help, Senator, if you'd like. But I think the basic difficulty is that Title III in its current structure protects the privacy of communications.

Here we are talking about trying to regulate something that is not necessarily a communication. When you have communications, you have parties and therefore you know whose consent you need or whose expectation of privacy the question should hinge on. So there is a structural difference between them.

Chairman SPECTER. Not withstanding the structural difference, you think Congress ought to be in it?

Mr. BANKSTON. Absolutely.

Chairman SPECTER. How about you, Mr. Zwillinger?

Mr. ZWILLINGER. Well, with due respect to Judge Posner and Mr. Bankston, I do think it makes sense to treat video differently.

If you think of one example, if the student's remote laptop could be turned on to intercept emails, we would want that to be illegal wherever the student is because they have a right to send a private email, even in a public place.

But with regard to video, we don't have a problem with the video being activated while the student is in the classroom or at the mall. We have problems when it is activated in the home or in the bathroom or in any other private place.

So I don't think Congress should stay out. I don't want you to misinterpret. I think Congress should stay out of putting video in Title III and Congress should focus on a narrow targeted statute

like the states have done to prevent video in private spheres without interfering with the ability to have a camera in an ATM or a camera in an elevator or even to turn on a webcam remotely in the office so employers can monitor in the office, just not at the home.

Chairman SPECTER. Professor Cate, would you keep the federal government out? Or should the federal government be legislating here?

Mr. CATE. Mr. Chairman, there is no question I believe the federal government should be legislating in this area. I would go far beyond what my colleague Mr. Zwillinger said because this is not just a question of location.

Location matters. We certainly feel special about bedrooms and bathrooms and changing rooms. But in the years in which, between when Judge Posner wrote and today, we have seen a proliferation of video cameras in every aspect of our lives.

We have the largest censored network in the world in the video cameras contained in cell phones. We have major investments by federal, local and state governments in video cameras on street corners, video cameras with extraordinary capabilities.

So, for example, facial recognition. So they say I know that that is Senator Specter walking down that street. We have linked video cameras so they can follow you from one street corner to the next.

When you go into your doctor's office, they can follow you in. They can link that together. We see major cities now, Chicago, for example, where private industry has linked its video cameras with government controlled cameras so that a government agent sitting in a bunker can access a business's cameras for the purpose of following people as they move.

In the workplace, the presence of cameras there while I certainly agree there may be a different expectation of privacy in the workplace, even the Supreme Court, no great friend of privacy, has found there is an expectation of privacy in the workplace.

So before an employer could turn on a camera that would surreptitiously record me in the workplace, presumably there should be some process there and that is process that I think Congress is in the best position to create.

Chairman SPECTER. Well, Professor Cate, as you described a hypothetical camera following a person through all the person's activities and to the doctor's office, to wherever he or she may go, that's a pretty ominous big brother scenario.

Mr. CATE. Yes, sir, Senator. I think it is quite ominous. I want to be clear.

Chairman SPECTER. Quite ominous.

Mr. CATE. Well, it is not, frankly, nearly as onerous as it is ominous because today the digital technology makes it much simpler now that we are beginning to link these cameras.

Moreover, many of these cameras, in fact the majority——

Chairman SPECTER. We are onerous and ominous. Would you amplify that?

Mr. CATE. Well, I think it is both a, it is a tremendous burden on civil liberties that individuals may effectively have no expectation of privacy. They may be identified, they may be linked to who they are talking to, they may be linked to where they are going. Even though many of those activities occur in public.

Chairman SPECTER. So you think it ought not to turn on an expectation?

Mr. CATE. I think it ought not to turn on a location. I think an expectation might be entirely appropriate. So that, for example, and as I suggested in my written statement, just as we define oral communications under Title III based in part on a reasonable expectation that a conversation will not be overheard, we could define video surveillance as occurring in an area where there is a reasonable expectation that one would not be the subject of video surveillance.

Chairman SPECTER. Well, if you say when you are walking down the street there is no expectation of privacy, if you say when you are in the elevator there is no expectation of privacy, certainly if you go into your doctor's office there is an expectation of privacy, but perhaps even in the circumstances where there is no expectation of privacy, if you aggregate them and put them all together and have a whole profile on a person, does that change the, is that a game changer?

Mr. CATE. Yes, sir. I believe it can be. I don't believe in every instance it must be, but I think that is the type of place where the protection of privacy would benefit enormously for some process around that so that we would say before an agent could do those things, we would like to know is there individualized suspicion, for example.

Let me just give you a very practical example. The Province of Ontario in Canada uses video surveillance extensively including on its public transportation, but they have a rule that they use a technology that obfuscates the face when the video is recorded and you can only get the technological screen removed from the face if you meet certain legal conditions.

So they have it, they are capturing it. It is all there. But they have protected it with a small technological protection which offers great privacy protection.

Chairman SPECTER. The comment was made about how many cell phones there are available. What is realistic to have some limitation, an enforceable limitation on cell phones?

There is a big sign in my health club, no cell phone cameras inside the premises. I had not thought of the cell phone camera beforehand, but there are so many. How do you deal with that? Mr. Richardson, do you care to venture?

Mr. RICHARDSON. Yes, Senator. In my own view, I think it's important, we have talked about the importance of place. I also think there is an opportunity to think about the context of the use of the device.

So while I don't think there is any effective way to legislate what people do with a cell phone that has a camera in it, I do think there are ways to legislate what they do with any video that they happen to take with those cameras and that the use of it either by the owner or by a third party could be determined in part by context. By that I mean if someone is using a work issued device whether it's a cell phone with a camera or a notebook, they could be clearly told that when they were using that in a workplace context that they might be monitored or the camera might be turned on.

I'm not saying that that would be good policy for a company, but it might be legal. In a sort of private workplace, not workplace, but personal environment, the use of that video captured capability without the consent of parties who appear in the video I think would be something that could be made unlawful.

Chairman SPECTER. Are there sufficient laws now to deal with the issue of pornography and videotaping?

Mr. RICHARDSON. Are you asking me, Senator?

Chairman SPECTER. Yes.

Mr. RICHARDSON. I would venture to say this. That with particular emphasis on child pornography, that is one area in the realm of computer security where there have been laudable results and a reduction in overall crime detection that the sort of single mindedness of purpose and the broad deployment of crime fighting capabilities worldwide really did see some results there.

Chairman SPECTER. So as to child pornography, you think we are, we have sufficient laws? Does anybody disagree with that? Professor Cate?

Mr. CATE. No, sir. I don't disagree with that.

Chairman SPECTER. Mr. Zwillinger.

Mr. ZWILLINGER. No, sir, I do not disagree.

Chairman SPECTER. Mr. Bankston.

Mr. BANKSTON. No disagreement.

Chairman SPECTER. Mr. Livingston.

Mr. LIVINGSTON. No.

Chairman SPECTER. There has been a bit of conversation on focusing on the right of privacy in the state of undress. Is that suggestive of a category of privacy where legislation might be directed to specific categories, undress being one and others like that specific situation which would limit the scope of legislation? Mr. Zwillinger, you are nodding in the affirmative?

Mr. ZWILLINGER. I am, Mr. Chairman. I do think that's a useful limiting principle because we think about what bothers us about video, we think about private spaces. When we think about truly private spaces, they are spaces in which we feel comfortable doing things like changing clothes.

It's not because the statute should only be geared towards voyeurism, it's because that defines a category of location where we are truly worried about privacy because we don't generally do that in public places. Change our clothes, that is.

Chairman SPECTER. Any other category come to mind, Mr. Zwillinger, like undress which would be one for specific inclusion?

Mr. ZWILLINGER. The other is the home certainly. Maybe you won't undress in your kitchen, but as the homeowner you certainly have a reasonable expectation that your home is sacrosanct, vis-a-vis third parties.

Chairman SPECTER. And how about your office?

Mr. ZWILLINGER. I think less so, Mr. Chairman.

Chairman SPECTER. Why?

Mr. ZWILLINGER. One of the problems with the case law about offices is employers also have an interest in protecting the security of their work space, protecting their employees, protecting their property.

So work spaces vary dramatically from federal government spaces with signs that say "everything may be monitored" to private companies with thousands of employees where they are monitoring product to small businesses like mine where we have ten employees.

So the circumstances are so different that trying to determine when somebody has a reasonable expectation of privacy in a hallway in front of an office, in a break area, in a kitchen, in an entranceway, it becomes very difficult to answer the questions that my clients ask in advance, which is "can I put up a camera here to prevent theft?"

So I think offices are different than homes and locker rooms and bathrooms.

Chairman SPECTER. Anybody disagree with the office?

Mr. BANKSTON. Yes, sir. I mean, I respectfully disagree to the extent that certainly the question of an expectation of privacy is often a case by case, very fact dependent inquiry. But it is the same type of inquiry that courts have been engaged in for over 40 years when considering electronic eavesdropping. It's not an insurmountable problem or something that people cannot prepare for.

I am less worried that people will be chilled from engaging in what would have been legitimate security video surveillance. Rather, I expect that a prohibition on video surveillance where there is an expectation of privacy would instead incentivize people to better notify those who are being put under surveillance.

Another point is I am wary of limiting our privacy protections based on whether we are in a state of undress or otherwise in a state of undress in that we don't distinguish in Title III when it comes to eavesdropping or wire tapping whether or not our conversations are particularly sensitive or what content they contain.

The question is whether these are private communications or not. Here the question is whether someone has an expectation of privacy that they are going to be photographed or not. I don't see why our privacy protection should turn on what amount of clothing we are wearing.

Mr. ZWILLINGER. Mr. Chairman, may I respond briefly?

Chairman SPECTER. Sure.

Mr. ZWILLINGER. You asked the question before about cell phones and the cameras that are ubiquitous in cell phone technology. When you did that, there are three things about that that relate to this debate.

The first was if I turn on someone else's cell phone, that's hacking, right? I'm hacking into their computer, hacking into their device so there may be adequate federal laws to cover that in the Computer Fraud and Abuse Act.

When I use my own cell phone, we have to be very wary of getting into First Amendment territory where we say it's illegal to take a video or picture without the consent of those who are photographed, because the First Amendment will also speak to that.

So when we are answering the question of why are we concerned in private spaces and not public spaces, our concern in public spaces is outweighed by other things. It is outweighed by the right to take film of what happens in public places for news reporting and it is outweighed by our notion that while we're concerned that

a camera might follow us to the doctor's office, we are much more concerned that the conversation with the doctor is private and the hierarchy of protection, the fact that I went to my doctor is somewhat below what I said to my doctor. That's true about priests and that's true about attorneys and that's true about everyone where we have a privileged relationship.

I'm sensitive to this and I'm suggesting that Congress target it, but in a more limited fashion than we treat some of these other things because there are unique differences in public spaces that don't exist in private spaces.

Mr. BANKSTON. To be clear, I'm not suggesting that we regulate the taking of photographs in public. We are, like Mr. Zwillinger, very sensitive to First Amendment concerns in this area and do not in any way want to hinder legitimate news gathering activity that takes place in public.

Mr. CATE. But Mr. Chairman, if I may, we currently apply Title III to prohibit the recording of conversations that take place in public if they take place with a manifestation of a reasonable expectation of privacy.

So in fact this would be cutting back on the existing protection we already have in Title III. So there are settings in public where we regard something that takes place there as being nevertheless private.

Of course the problem is categorizing. So even the state of undress, but if you have been to a beach recently, there is a great deal of state of undress going on there. So we would have to use these categories as a way of demonstrating I think a broader principle, namely the one already reflected in the law, a reasonable expectation of privacy so that a person undressing in a dressing room with a door around it would have an arguably reasonable expectation of privacy. A person undressing on a beach would presumably not have a reasonable expectation of privacy.

It would not be determinative by whether they were undressing or by where they were located. It would be all of the circumstances that answer the reasonable expectation of privacy question.

Chairman SPECTER. Professor Cate, the Supreme Court will soon hear argument in *City of Ontario* v. *Quon*, the case in which the Ontario California police department read text messages on papers given to its SWAT officers without a warrant.

Will the Supreme Court's ruling in that case, which concerns employee privacy rights in the workplace, have any applicability on the issues which we have discussed today?

Mr. CATE. I don't think so, Mr. Chairman. Again, because what we have been talking about today is primarily a vacuum in current law, and what the Supreme Court will be talking about is the application but of a clearly defined area of law.

I would add, our conversation is largely focused on this as if it is a binary issue. You either can or you can't. But practical experience has demonstrated rarely does Title III result in a binary result, either yes or no.

So, for example, the audio monitoring, the oral conversation monitoring provisions have led businesses that do audio monitoring to put warnings in their windows to say we do audio monitoring,

thereby defeating the reasonable expectation of privacy so that it's legal for them to do it.

It's not that they are prohibited from doing it, it is that they have to comply with some reasonable standard in order to do it.

Mr. RICHARDSON. Mr. Chairman, if I might.

Chairman SPECTER. Go ahead, Mr. Richardson.

Mr. RICHARDSON. I would say with due respect that the Ontario California case may have some bearing here precisely because it relates to a case, the expectation of someone using an institutionally owned device in their private lives. I think that that is one area of expectation and I agree with my colleagues that expectation in terms of privacy is an important element.

But I think as a practical matter increasingly people use, they don't want to carry two cell phones and so they tend, I mean, some of you may have to right now, but they do tend to intermingle regular life so to speak and their work lives.

I don't think there is any way in today's world to disentangle those. So the context I think determines to some degree the expectation of privacy. The thorny part for institutional owners of these devices is how they can protect their own interests while still allowing and not getting involved in personal business that may be conducted on those devices.

Chairman SPECTER. Mr. Cate, you have to depart shortly for a plane and we want to respect that.

I want to get an idea from each of you experts as to at least the four of you who have said that the federal government should get into the picture, what would you propose that the federal legislation provide?

Mr. CATE. Well, thank you very much and I apologize again for having to leave this very interesting discussion early.

I would have to say that I am agnostic over the question of whether the legislation should address video surveillance within Title III or whether it does it in a separate piece of legislation.

Chairman SPECTER. How does being agnostic affect that?

Mr. CATE. Well, I certainly understand the argument why it would be better addressed in a separate piece of legislation.

Chairman SPECTER. Which way would you go? We have plenty of paper.

Mr. CATE. On the other hand, I think it is very difficult to get anything new passed through Congress. So amending an existing law strikes me as more likely to succeed and given that we've been at this for 25 years, it is time we need this change in the law. So I would be happy to see an amendment to Title III.

I suggested one possibility in my written testimony to mirror the definition of oral communications but instead use it for video surveillance. I think there are other excellent approaches, but I think it can be done and I think it's time to do it.

Chairman SPECTER. Mr. Zwillinger, how would you approach legislation?

Mr. ZWILLINGER. I think I would commend the Delaware statute as a potential model. The Delaware state statute, one of the states that has taken on this issue, has passed a statute that does two things.

It makes it a crime to capture without the consent of the person, the image of a person who is getting dressed or undressed in specific locations where persons normally disrobe and they have a reasonable expectation of privacy and it makes it a crime to install video surveillance in a private place without the consent of the people entitled to an expectation of privacy there.

So it's limited by place in one aspect and the other aspect is limited by intent, the voyeuristic intent. I think that is the type of narrow targeted approach that if there is a federal hook for interstate commerce nexus that the federal government should consider.

Chairman SPECTER. Mr. Bankston.

Mr. BANKSTON. Unlike Mr. Cate, I'm not agnostic in terms of which statute would be the best home for something covering video surveillance. I do think Title III is the appropriate home if only because the courts have already been applying Title III's requirements in terms of law enforcement video surveillance.

Like Mr. Cate, I think that the appropriate approach would be analogous to the way the statute currently handles oral communications hinging on one's expectation of privacy as to whether one will be photographed as opposed to recorded in terms of oral communications.

Yes, so that's basically it. I think Title III should be amended to cover this conduct. I think that oral communications are the best analogy here. There will be some difficulties in mapping the video surveillance onto Title III because these are not communications and they do not have parties. But difficulty in drafting should not be a reason to not do this because it has been a quarter of a century and it is time to get the job done.

Chairman SPECTER. And Mr. Richardson, what would your thinking be as to how to approach the statute.

Mr. RICHARDSON. Well, I think it may be somewhat to my credit that I'm not a legal expert, but to my way of thinking, the distinction made between oral and video interception of communications is a bit of a red herring, particularly when it comes to surveillance on devices like mobile computers.

In the Lower Merion case, so far as we know, no audio was recorded, but as a practical matter generally when you turn on the webcam in a notebook, the audio does turn on. There may have been a choice on the receiving end and the storage end only to store one still frame, but almost certainly what was sent upstream across the Internet was video with audio.

So trying to draw a distinction about whether that, what form that data took I think is probably misguided and I would agree with my colleagues that expectation and context are the relevant factors.

Chairman SPECTER. Mr. Livingston, your work as you have noted is on recovery for property. Without getting unduly into the Lower Merion situation, there has been the thought that there is justification in the context of stolen laptops taken off premises with the intent not to return, whether that would be sufficient justification for turning them on to identify what has happened to them for purposes of recovering the property.

Do you think that is a sufficient basis as a generalization for activating them and having whatever happens with respect to privacy happen?

Mr. LIVINGSTON. In our framework we work with law enforcement. We do require the owner of the device that has been stolen to register that theft report with law enforcement and that begins the recovery process.

Fundamentally we are most always working with stolen devices reported to Law Enforcement so we don't believe the unauthorized user of the device has any expectation of privacy at that point.

Chairman SPECTER. I am advised that Mr. Robert Wegbreit is in the audience, a parent of a student from the Lower Merion school district. Is Mr. Wegbreit present? Would you care to step forward?

Since you are here on this subject, have a chair. Would you care to make a statement?

Mr. WEGBREIT. Sure. My name is Bob Wegbreit.

Chairman SPECTER. You are not compelled to make a statement.

Mr. WEGBREIT. That's fine.

Chairman SPECTER. It is if you are interested and willing to make a statement.

Mr. WEGBREIT. I am willing to make a statement.

Chairman SPECTER. I just didn't want to have you in the room without having the opportunity to say something if you wanted to do so.

**STATEMENT OF ROBERT WEGBREIT, PARENT, LOWER MERION SCHOOL DISTRICT**

Mr. WEGBREIT. My name is Bob Wegbreit. My daughter, Anna Wegbreit, is a student at Harriton High School, one of Lower Merion school district high schools.

Chairman SPECTER. When Strom Thurman used to preside over hearings like this, he would say pull the machine a little closer.

Mr. WEGBREIT. Thank you. First of all, Senator, thank you very much for holding this. It is a very important issue for our community.

When this occurred, myself and three other parents formed a group, LMSDparents.org to see what the other parents felt about this. Since then, we have communicated with over 500 of the probably 1,800 or 1,900 families who have students at Lower Merion high schools.

Overwhelmingly, the conversation was that we have excellent schools, that we want our children and other students throughout the country to have access to excellent technology and cutting edge technology.

We also trust our educators, our administrators, our school board to the point that they have the best interest of our students' education and our students' welfare at heart. You would be surprised that unlike the headlines, if something truly damaging did occur to our students, however, the concern of what privacy breaches did occur were common throughout the comments that we have gotten from many of these parents.

How do we protect and prevent this from happening with these type of privacy laws to our children?

This morning I asked my daughter, if you knew that the webcams could be activated, what would we, what would she have done different? I'm very fortunate that she said daddy, I don't do anything inappropriate. However, that's not the answer that we need to look to as a community.

I think the parents of the families that were affected learned that perhaps the webcam was activated in their household, they want it almost like cigarettes with a warning so that we can respond properly. But at the same time, like cigarettes we must recognize the second hand smoke concept that surveillance that occurs beyond the intended surveillance and is not anticipated by others in the room, in the property who have expected privacy, that must be addressed also.

So those are the concerns of the community as we look at why was there a camera potentially on in our household but we didn't know that would have happened? At the same time we don't believe that our school district is anything but an excellent place to have our children educated. Thank you.

Chairman SPECTER. Would you like to see federal legislation on this subject?

Mr. WEGBREIT. I would, because then we would all know where everything stands. What that legislation says, if the school district mandates my child have a laptop with a webcam and that they can turn that on at anytime, I don't agree with that, but at least we know and recognize it, we would maintain that laptop in a very specific area of the house which might be better than my daughter being in her bedroom on the laptop all evening.

But we would know that and I think that's what the consistent tone of the parents that I've spoken to, I've been very fortunate to hear from so many of them both in personal communication and emails and signing a petition. They trust that the district knows what is in the best interest of our children, but we want to know what that interest is.

Chairman SPECTER. Thank you very much, Mr. Wegbreit.

Mr. WEGBREIT. Thank you.

Chairman SPECTER. We appreciate you being here. Let me go back to some broader questions with this group of experts here on, so much is swirling around in the news on cyberspace. What should we be doing to protect cyberspace? We see comments by the Secretary of Defense, Robert Gates, about the United States being at risk on invasions of cyberspace.

Are any of the issues which we have discussed here today relevant on that subject? Mr. Zwillinger?

Mr. ZWILLINGER. Well, in many ways it is a much broader topic than the question for the hearing. There are lots of things that we need to be doing to protect cyberspace and one of those things, one of those easy things is making cyberspace security a real focus of research and development and career technology in developing and putting America's smarts to work in a field that has for too long not been the number one priority in the country.

So cybersecurity is a topic that is near and dear to my heart and there has been some federal legislation that has been proposed over time that makes some sense.

The question that you've asked is a difficult one as to what extent this relates to that. I think that goes back to some of my opening remarks that we have an issue with trying to strike the right balance between privacy and security and despite Mr. Bankston's and my disagreement about the mechanism about Title III, we generally agree that for too long in many places that balance has been towards security.

In cyberspace, we have a deficiency in both areas. That is our statutes aren't updated to protect privacy the way we would like in the cloud computing sphere when our data is stored with remote providers and our security posture is not where we would like it as well.

I don't think that turning on or turning off remote video monitoring has anything to do with the need to secure our cyber infrastructure.

One might think the more security you can have the better, but I don't know that remote video would help recover the laptop, I don't know that remote video helps us determine who the foreigners who may be attacking U.S. computer systems are.

We can't turn on their videos, and if we could, I don't know what we'd learn from that. So it's a very difficult question, but I think cybersecurity and privacy in cyberspace are two priorities that we need to work towards together.

Chairman SPECTER. Well, when we pick up the privacy issue, of course it is a totally different dimension on privacy, but that is what comes to mind. Any thinking on this, Mr. Bankston?

Mr. BANKSTON. A couple of points. In one factual way, this is relevant to cybersecurity to the extent that laptop cameras and microphones pose another vulnerability. There was a story that was cited in my written testimony describing how a particular U.S. government website when visited would exploit vulnerabilities in Microsoft's web browser to install software that could among other things be used to activate a camera.

But the broader and I think more important light that this sheds on the cybersecurity debate is that where there is surveillance capability, it can be abused. So I think it is very important in the cybersecurity bill that was just marked up in the Commerce Committee, there were clear delineations of what the President's power was, in particular making sure that the President in his authority to create and execute a cybersecurity emergency plan was not given any kind of express or implied exception to or authorization beyond the wire tapping and stored communications statutes.

So the broader point, surveillance power can be abused and in dealing with cybersecurity, we need to be clear in our protections in terms of surveillance such that in securing our national infrastructure we do not also violate the privacy of American citizens.

Chairman SPECTER. Mr. Richardson, care to venture into this field?

Mr. RICHARDSON. With pleasure. I think that cybersecurity is an area where we have in several instances better technology than we have deployed and part of the reason for that lack of deployment is lack of incentive. There isn't sufficient fear of liability or inadequate security as one example. So there may be opportunities to apply some legislative pressure to improve that situation.

Additionally, I have long been an advocate of a better framework for identity management on the internet than simply the knowledge of who is engaging in any activity on the internet and I think that that helps create deterrents.

The problem with it of course is that it also raises serious privacy concerns. There are I think ways to deal with that, but these are areas that are very murky in current legislation. So as it relates specifically to the issue of surveillance and video surveillance, it is clear that in the current environment that there will be and surely already is abuse.

Solving some of the broader problems of cybersecurity may help curb that abuse as well.

Chairman SPECTER. Mr. Livingston, would you care to comment on this subject?

Mr. LIVINGSTON. No, Senator. I will leave it to the other experts. Thank you.

Chairman SPECTER. Okay. One other subject which is in the stratosphere. All this battle between China and Google, while we are talking about the subject, there is a lot of wonderment by nonexperts in the field.

Mr. Zwillinger, dealing with China is a big, vast subject all by itself of which I'm doing a lot of work on with the International Trade Commission on unfair trade practices where China violates the international trade laws, takes our jobs, takes our money, loans it back to us. It's a big part of the United States now.

You have this battle royal between Google and China. Maybe Google is the right entity to fight China as opposed to anybody else.

What in this whole field of the internet and cyberspace would be applicable to maybe some evaluation as to what's happening with China or Google? Mr. Zwillinger, any thoughts?

Mr. ZWILLINGER. One of the difficulties which is not China specific but deals with any U.S. company that goes abroad to offer its communication services is how it reconciles the need to follow the rules of the local government and the local space with the American principles about when data should be turned over and when it should be exposed.

When you do business with China and Vietnam and other places, there comes a question of when companies like Google should turn over data. If you don't obey the local law enforcement and the local processes, you subject people there to problems, and if you do, you do things that maybe you wouldn't do in the United States.

So it seems to be very difficult to take a topic that we struggle with which is privacy and security and try to export them to other countries without significant consequences and difficulty.

I think what Google is struggling with is a combination of all those things. It's a combination of when do they listen to the Chinese government and when do they not and when do they turn off their entire system to people from China as a step to tell the Chinese government that we don't approve of your behavior.

I recognize the difficulty of the question. I'm not sure I can give you any help in answering it.

Chairman SPECTER. Any thinking on that, Mr. Bankston.

Mr. BANKSTON. I mean, I guess certainly the China situation highlights the difficult role of communications intermediaries both in terms of maintaining their user's privacy and protecting their user's ability to express themselves in the face of a government that may not always be friendly to either of those ideas.

I think it should reflect also on the fact that the companies are in the same situation here in the United States. Not to analogize the United States government to the Chinese government, but certainly even companies here are often placed in an awkward and difficult situation trying to balance the needs of their users and the privacy rights of their users with the requests of the government.

So I think that one thing we need to look to here which we can't expect from China but we should expect from ourselves is greater transparency in terms of how the government accesses communications data from companies here in the United States.

Looking at Title III for example, it is the one of the major electronic privacy statutes that requires any meaningful reporting about when the government is engaged in this kind of conduct.

So we know when the government is wire tapping. We don't know, for example, when the government is acquiring search queries from Google or acquiring stored email or doing any other kind of surveillance that isn't wire tapping itself.

So I think we should look for transparency here in the United States which we certainly won't be seeing from governments like China.

Chairman SPECTER. Thank you. Mr. Richardson.

Mr. RICHARDSON. Mr. Chairman, I think that if you will recall the Google incident first came to light because Google felt that they had been attacked by some entity in China. They were unwilling to go so far as to venture to say that it was the Chinese government that was responsible. I don't think any of us here is in a position to say one way or the other.

What is clear is that Google reacted as if that were the case. Their response was made to the Chinese government, or how they would conduct business in China. As such, what struck me was that these were attacks that were carried out against internet resources and infrastructure in the U.S. and in that U.S., largely the infrastructure that we are discussing today is privately owned.

Therefore, the role of the government in dealing with these kinds of attacks is at this point somewhat unclear. I think in this instance it certainly appeared to me that the Department of State, for example, was caught somewhat flat footed. I didn't get the impression that they had been briefed that Google was going to come out in force before it happened.

That kind of coordination I think is going to be increasingly important where the federal government makes clear its role, and of course the new legislation that has just been marked up I think does go some ways to addressing that.

But when it comes to cyber relations as it were between government entities, there is I think a great deal of work to be done in defining what our federal posture is.

Chairman SPECTER. Thank you, Mr. Richardson. Any comment on that, Mr. Livingston? Or final comment?

Mr. LIVINGSTON. Senator, we have recovered computers in about 50 countries around the world. We haven't had a lot of experience with China, but we'd be happy to report back at some future date if and when we do.

I'd just like to say that if there was a Title III new legislation that was considered, I would hope that there would be an exception for devices that were stolen. Again, we don't believe that somebody in possession of stolen property necessarily has an expectation of privacy.

Chairman SPECTER. Without objection, I will place in the record a statement by Mr. Blake J. Robbins concerning the, as he puts it, the laptop embedded internet camera capable of activation while in students' homes and it is pressing the view "as technology continues to improve at light speed, the need to protect the sanctity of our home from invasion grows even more urgent. Consequently, we earnestly support legislation that will govern against and punish the misuse of any technology that would prevent any such electronic invasion."

From Mr. Blake Robbins. His mother, Holly Robbins, his dad, Richard Robbins, and his sister, Paige Robbins. That is a statement for the record from plaintiffs in the litigation.

The testimony in my opinion has been very forceful on the point of a need for legislation. There is no doubt that there is a gap in existing federal law. The language of the constitution itself of the Fourth Amendment is in my judgment not sufficient. It was not sufficient for oral or wire tap information which led Congress to legislate under Title III.

This Senator will accept the invitation of Judge Posner to legislate. I will be drafting legislation to introduce into the Senate to try to carry the gap which now exists. I think the testimony has been very forceful and we have tried to steer away from the Lower Merion situation, but when the gentleman is present in the courtroom, in the hearing room, I thought it appropriate to have him testify briefly and to put into the record the statement of one of the students of the family expressing the concern and looking for protection for privacy.

Without any doubt, privacy is a very highly valued American value. It is a value of the utmost importance. My sense is that my colleagues will be responsive and have been alerted by this specific incident. But beyond that as the testimony of this very distinguished panel has demonstrated, there is a gap and it ought to be closed. After 25 years, it is time.

That concludes our hearing. I appreciate your coming in. Thank you.

[Whereupon, the hearing was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

**Electronic Frontier Foundation**

**Statement of Kevin S. Bankston**
**Senior Staff Attorney**
**Electronic Frontier Foundation**

**before the**
**U.S. Senate Committee on the Judiciary**
**Subcommittee on Crime and Drugs**

**for the field hearing on**
**Video Laptop Surveillance: Does Title III Need to Be Updated?**

**Philadelphia, Pennsylvania**
**March 29, 2010**

454 Shotwell Street, San Francisco, CA 94110 USA
+1 415 436 9333 (v) +1 415 436 9993 (f) www.eff.org

Statement of Kevin S. Bankston

## I. INTRODUCTION

Chairman Specter, Ranking Member Graham, and Members of the Subcommittee, thank you for giving the Electronic Frontier Foundation[1] (EFF) the opportunity to address the question raised by today's hearing: should the federal wiretapping statute be updated to regulate secret video surveillance, just as it restricts electronic eavesdropping?

EFF's answer to that question is a definitive yes. We live in a modern age of ubiquitous networked cameras such as "web cams", which bring with them a risk of secret video spying that is unprecedented in scope. Title III of the Omnibus Crime and Control Act of 1968 as amended by the Electronic Communications Privacy Act (ECPA) of 1986, otherwise known simply as the Wiretap Act, currently only regulates electronic eavesdropping on oral conversations and the interception of voice and electronic communications. There is no reason why Congress should not amend that law to also provide Americans with equally strong privacy protections against surreptitious video surveillance.

## II. ALLEGATIONS OF LAPTOP WEB CAM SPYING IN THE LOWER MERION SCHOOL DISTRICT

Recent events in Pennsylvania's Lower Merion School District have put the spotlight on how Americans are at risk of being secretly photographed in the privacy of their own homes—even in the privacy of their own bedrooms—using laptop web cams accessed and controlled remotely by other parties.[2] Last month, right here in the U.S. District Court for the Eastern District of Pennsylvania, the parents of Harriton High School student Blake Robbins filed a class action lawsuit against the school district on behalf of their son and other students in the district, based on the shocking allegation that school administrators have secretly used the web

[1] EFF is a non-profit, member-supported public interest organization dedicated to protecting privacy and free speech in the digital age. For more information on EFF, visit http://www.eff.org.

[2] This testimony does not address the issue of video surveillance conducted in public spaces.

cams in school-issued laptops to photograph students even after they have taken their laptops home from school.[3] According to the complaint, Blake Robbins first learned of the alleged laptop spying this past November when an assistant principal stated her belief that Blake was engaged in improper behavior in his home, citing as evidence a photograph from Blake's laptop. According to more recent interviews with Blake and his attorney, school officials suspected that Blake was involved in illicit drugs because he was allegedly photographed holding pill-shaped objects; the Robbins family maintains those "pills" were simply Mike-N-Ike candies, a favorite of Blake's.[4]

After the lawsuit was filed, LMSD's Superintendent of Schools, Dr. Christopher W. McGinley, issued a series of letters[5] to district parents explaining the school district's side of the story. McGinley admitted that school administrators did indeed have the capability, through the theft-tracking features of security software[6] installed on students' laptops, to remotely take pictures using the laptops' web cams.[7] McGinley further claimed that the feature was only ever activated when a laptop was reported

---

[3] Full complaint *available at* http://www.scribd.com/doc/27077604/LMSD-Laptop-Spying-Court-Docket-Filed-2-11-2010.

[4] *See* Vince Lattanzio, Webgate Teen: "I Hope They're Not Watching Me", NBC PHILADELPHIA, Feb. 22, 2010, *available at* http://www.nbcphiladelphia.com/news/tech/WebcamGate-Teen-I-Hope-Theyre-Not-Watching-Me-84826357.html.

[5] Letter of Feb. 18, 2010 *available at* http://www.lmsd.org/sections/news/default.php?m=0&t=today&p=lmsd_anno&id=1138, letter of Feb. 19, 2010 *available at* http://www.lmsd.org/sections/news/default.php?t=today&p=lmsd_anno&id=1143

[6] The software in question is the TheftTracker feature of the LANRev security software package, now called Absolute Manage by the software's new owner, Absolute Software. In light of the Lower Merion controversy, the company published a blog posting stating that the feature allowing for remote activation of the web cam would be removed from the next version of the software, concluding that "webcam pictures are not a useful tool in tracking down the location of a stolen computer." *See* Stephen Midgley, *Lower Merion School District and Do-It-Yourself Recovery Solutions*, ABSOLUTE SOFTWARE LAPTOP SECURITY BLOG, Feb. 23, 2010, *available at* http://blog.absolute.com/lower-merion-school-district-and-do-it-yourself-recovery-solutions/.

[7] An earlier promotional video of a Lower Merion School District staffer demonstrating the TheftTracker software was posted to Youtube after the laptop web cam controversy arose, *available at* http://www.youtube.com/watch?v=oLB4LNFybFI.

lost or stolen, although notably, the Robbins allege that Blake's computer was never reported lost or stolen. Finally, McGinley admitted and apologized for the fact that no formal notice of the functionality or use of the remote picture-taking feature was ever given to students or the families.

More recent news stories indicate that rather than simply failing to give notice, the school may have been actively concealing its ability to remotely activate the laptop cameras. Several students have come forward claiming that they had noticed in the past that the green LED lights that illuminate when their laptop web cams are in use would occasionally turn on, seemingly at random. According to these students, when they asked school officials about this, they were told that the behavior just a "glitch".[8]

Whether or not all of these frightening claims are true, the controversy over the school district's previously secret capability to surreptitiously photograph students in their homes—a controversy that some students have dubbed "Webcamgate"[9]—has highlighted the significant privacy risk posed by web cams.

Web cams unquestionably represent an awesomely useful technology, giving millions the ability to privately and instantaneously have video-enhanced conversations with others, be they across the street or on the other side of the planet. However, this awesome technology carries with it an awesome new privacy risk. With millions upon millions of laptop web cams routinely being carried into the home and other private spaces, surreptitious video surveillance has become a pervasive threat. This threat is exponentially greater than the threat posed by secret videotaping in 1968 when Title III was originally passed or even in 1986 when the law was updated to cover the interception of electronic communications.

---

[8] *See* Robert Mackey, *School Accused of Using Webcam to Photograph Student at Home*, THE LEDE: THE NEW YORK TIMES NEWS BLOG, Feb. 19, 2010, *available at* http://thelede.blogs.nytimes.com/2010/02/19/school-accused-of-using-webcam-to-photograph-student-at-home/.

[9] *See* Dan Hardy, Lydia Woolever, and Joseph Tanfani, *Subpoena Issued in L. Merion Webcam Case*, PHILLY.COM, Feb. 20, 2010, *available at* http://www.philly.com/philly/news/homepage/20100220_Subpoena_issued_in_L__Merion_webcam_case.html.

Put simply, any camera controlled by software on a computer or mobile device that is connected to the Internet carries the risk that the camera will be remotely activated without the knowledge or consent of the user, whether by stalkers, computer criminals or foreign governments using "malware" to break into and take control of the camera, [10] or by schools or employers with access to the computer, or even by government investigators attempting to monitor a suspect.[11]

Yet, American citizens and consumers lack the most basic protections against this kind of spying. In particular, manufacturers have failed to give us basic technical protections, such as lens caps and hard-wired on/off power switches for the cameras, so we can all be sure that when we've turned off our web cam, no one else will turn it on. In the meantime, we recommend that laptop owners do what many of the students in Lower Merion are doing—cover your camera lens with a piece of tape or a post-it note.

More importantly for the purpose of this hearing, Americans also lack any meaningful federal legal protection against this kind of secret, unconsented video surveillance of private spaces.

---

[10] *See* Larry Magid, *Many Ways to Activate Webcams Sans Spy Spoftware*, CNET NEWS: SAFE AND SECURE, Feb. 22, 2010, *available at* http://news.cnet.com/8301-19518_3-10457737-238.html (describing various methods by which web cams can be remotely controlled by unauthorized users, including a description of how a Chinese government web site was configured to exploit a security vulnerability in Microsoft's Internet Explorer 6 web browser and infect visiting computers with "malware" that allowed for remote control of the computers' web cams).

[11] For analogous scenarios of the government remotely installing software on a suspect's computer to monitor Internet transmissions and remotely activating the microphone on a suspect's cell phone, *see* Declan McCullagh, *FBI Remotely Installs Spyware to Trace Bomb Threat*, CNET NEWS: NEWS BLOG, July 18, 2007, available at http://news.cnet.com/8301-10784_3-9746451-7.html, and Declan McCullagh, *FBI Taps Cell Phone Mic as Eavesdropping Tool*, CNET NEWS, Dec. 1, 2006, *available at* http://news.cnet.com/2100-1029_3-6140191.html.

## III. TITLE III'S CURRENT INAPPLICABILITY TO VIDEO SURVEILLANCE

The Lower Merion School District web cam controversy should be Congress' wake-up call to address a troubling gap in federal privacy law: as legislative history makes clear and as every court to address the question has held, Title III does not in any way prohibit or regulate such video surveillance.

Title III as amended by ECPA,[12] otherwise known as the Wiretap Act, creates criminal and civil liability for the interception—in other words, the acquisition by a device—of any oral, wire, or electronic communication without the consent of a party to that communication. "Oral communications" are essentially spoken words that are uttered by someone with a reasonable expectation that they won't be recorded. "Wire communications" are also spoken or otherwise aural communications, but only those that are transmitted over the Internet, the telephone network or the like. "Electronic communications" are any transmitted communications that are not wire communications, whether they contain text, images, sound, or any other sign or signal. Unless you are a party to a communication, or have the consent of a party, intercepting any oral, wire or electronic communication without court authorization is both a felony crime and a civil wrong carrying stiff statutory damages.

So, for example, secret monitoring of your email transmissions, wiretapping of your telephone calls, or secret eavesdropping using a microphone hidden inside your home would all violate Title III. However, the secret use of a web cam or a radio-controlled camera to photograph you inside your home is not currently regulated or prohibited by Title III, because in such a case there would be no oral, wire or electronic communication of yours to be intercepted. The only communications would be the electronic communications between the camera and the person who is remotely operating it, and that person is a party to those communications as opposed to a third party intercepting your communications with someone else. So, even though such secret video surveillance can be just as invasive

[12] Codified at 18 U.S.C. § 2510 *et seq.*

if not more invasive than listening in on your conversations or monitoring your telephone or Internet communications, Title III simply doesn't apply.

In 1984, the Seventh Circuit was the first appellate court to consider whether Title III regulates secret video surveillance, in the case of *United States v. Torres*.[13] There, the FBI had installed both eavesdropping and video surveillance equipment inside an apartment being used by members of a domestic political group suspected of involvement in several bombings.[14] The FBI had done so based on a court order issued under Title III, and the defendants argued that the video evidence used at trial should have been suppressed because Title III did not authorize such video surveillance, but rather forbade it.

In an opinion by Judge Posner, the Seventh Circuit agreed with the defendants—but only to a point. Looking to the language of the statute, the Court concluded that the video surveillance did not "intercept" any communication, and therefore held that Title III neither authorized nor prohibited the surveillance.[15] Looking beyond the statute's plain language, the Court further noted that the Wiretap's Act's legislative history did not mention video surveillance at all, "probably because television cameras in 1968 were too bulky and noisy to be installed and operated surreptitiously."[16] Such cameras obviously posed a greater privacy threat in the 1980s, and today pose a pervasive threat reaching nearly every laptop owner.

In *Torres*, the Seventh Circuit Court of Appeals flatly concluded that Title III did not authorize or regulate video surveillance.[17] However, the court further found that Rule 41 of the Federal Rules of Criminal Procedure, which governs the issuance of search warrants, did give courts the authority to issue warrants authorizing such video surveillance—with one very important caveat. The court held that in order for such a warrant to be constitutional under the Fourth Amendment's prohibition against

---

[13] 751 F.2d 875 (7th Cir. 1984), *cert. denied*, 470 U.S. 1087 (1985).
[14] *See id.* at 876-77.
[15] *See id.* at 880.
[16] *Id.* at 880-81.
[17] *Id.*

unreasonable searches and seizures, the warrant must be issued under the procedures of Title III that ensure that surveillance is narrowly targeted, those procedures representing Congress' best attempt to codify the Supreme Court's previous Fourth Amendment decisions regarding electronic eavesdropping. [18] In essence, although finding that Title III did not apply to video surveillance, the *Torres* court borrowed provisions of that statute meant to ensure the "particularity" of the surveillance in order to define how a court may issue a warrant under Rule 41 for video surveillance of private spaces that is consistent with the Fourth Amendment.[19]

Since the *Torres* decision, each of the six other appellate courts to consider the same question, including the court in this Circuit in an opinion authored by now-Chief Justice Alito, has arrived at the same answer: Title III does not prohibit or regulate video surveillance, but courts must follow its procedures when issuing warrants for such surveillance to ensure that the Fourth Amendment is not violated.[20]

---

[18] *Id.* at 883-86.

[19] As the *Torres* court explained,

> [T]he judge must certify that [1] "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," 18 U.S.C. § 2518(3)(c), and that [2] the warrant must contain "a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates," § 2518(4)(c), [3] must not allow the period of interception to be "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days" (though renewals are possible), § 2518(5), and [4] must require that the interception "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under [Title III]," *id.* Each of these four requirements is a safeguard against electronic surveillance that picks up more information than is strictly necessary and so violates the Fourth Amendment's requirement of particular description.

*Id.* at 883-84.

[20] *See United States v. Biasucci*, 786 F.2d 504, 508-10 (2d. Cir. 1986), *cert. denied*, 479 U.S. 827 (1986) (video surveillance of private offices), *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251-52 (5th Cir. 1987) (video surveillance of defendant's backyard from a video camera installed atop a power pole overlooking the 10-foot-high fence bordering the yard), *United States v. Mesa-Rincon*, 911 F.2d 1433, 1436-39 (10th Cir. 1990) (video surveillance of private warehouse), *United States v. Koyomejian*, 970 F. 2d 536, 538-42

Although those decisions were typically in the context of an appeal of the denial of a motion to suppress video evidence in a criminal case, the *Torres* court's logic has been followed in civil cases as well, most notably in this very courthouse in 2000. In that case, *Audenreid v. Circuit City Stores, Inc.*,[21] the court for the Eastern District of Pennsylvania held that an employer's use of a silent video surveillance system in an employee's office did not violate the Wiretap Act or Pennsylvania's wiretapping statute because it did not record sound.

## IV. CONGRESS CAN AND SHOULD UPDATE TITLE III TO PROHIBIT AND REGULATE VIDEO SURVEILLANCE

As Judge Posner rightly observed back in 1984, before laptops and web cams even existed:

> *Of course* it is anomalous to have detailed statutory regulation of bugging and wiretapping but not of television surveillance, in Title III...and we would think it *a very good thing* if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope.[22]

EFF agrees with Judge Posner on this score: of course it is anamolous that Title III does not cover video surveillance, and it would be a very good thing for Congress to update the law accordingly.

Over 25 years have passed since Judge Posner recommended such a change but Congress has yet to act, even though the threat of surreptitious video surveillance has increased exponentially along with the number of Internet-connected cameras that are vulnerable to outsiders' exploitation. Congress had its best chance in 1986, shortly after *Torres*, when it passed the Electronic Communications Privacy Act to amend Title III to cover the

---

(9th cir. 1991) (*en banc*), *cert. denied*, 506 U.S. 1005 (1992) (video surveillance of private offices), *United States v. Falls*, 34 F.3d 674, 678-80 (8th Cir. 1994) (video surveillance of apartment), and *United States v. Williams*, 124 F.3d 411. 416 (3rd Cir. 1997) (video surveillance of private office).

[21] 97 F.Supp.2d 660, 662-63 (E.D.Pa. 2000).

[22] *Torres*, 751 F.2d at 885.

interception of electronic communications as well as oral and wire communications. However, as the legislative history makes clear, Congress expressly chose not to do so,[23] even though Congress was aware of and expressly condoned the courts' approach of applying Title III's core requirements to warrants for video surveillance.[24]

Congress' regrettable and somewhat baffling failure to regulate video surveillance in 1986 has been made all the more regrettable by a vastly changed technological landscape that is now filled with miniature, networked cameras that can be turned to good purpose or to ill. We at EFF are therefore thankful to this Committee for taking up the issue and re-examining the question of whether Title III should be updated to regulate video surveillance, because—to put it bluntly—the inapplicability of Title III to video surveillance simply makes no sense.

It makes no sense that if the Lower Merion School District's administrators had eavesdropped on students conversations at home using the laptop's microphone, or had intercepted a student's private video chats,

---

[23] The ECPA Senate Report clearly notes that the amended statute does not apply to video surveillance:

> [T]his bill does not address questions of the applications of Title III standards to video surveillance and only deals with the interception of closed-circuit television communications [such as video teleconferencing] . . .. [I]f law enforcement officials were to install their own cameras and create their own closed-circuit television picture of a meeting, the capturing of the video images would not be an interception under the statute because there would be no interception of the contents of an electronic communication. Intercepting the audio portion of the meeting would be an interception of an oral communication, and the statute would apply to that portion.

S. REP. NO. 541 at 16-17 (1986). A bill specifically amending Title III to cover video surveillance was introduced by Congressman Kastenmeier, one of the drafters of Title III, but no action was taken on the bill after it was referred to committee. *See* The Video Surveillance Act of 1987, H.R. 1895, 100th Cong. (1987), summary of bill and legislative action available at http://thomas.loc.gov/cgi-bin/bdquery/z?d100:HR1895:.

[24] In ECPA's legislative history, Congress approved of the courts' approach as providing "legal protection against the unreasonable use of newer surveillance techniques." H.R. REP. NO. 99-647 at 18, 18 n.11 (1986).

they would clearly be guilty of a felony violation of Title III, but surreptitious video surveillance alone is not regulated by the statute at all.

It also makes no sense that a public school or any other government entity that wanted to legally spy on a student in this manner would have to get a prosecutor to obtain a probable cause warrant that satisfies Title III's core requirements in order to comply the Fourth Amendment, yet a private school could do so without any regard to Title III at all.

Finally, it makes no sense that Congress, while strictly regulating electronic eavesdropping on people who have a reasonable expectation of privacy that they won't be recorded, would leave the regulation of equally invasive video surveillance up to the states. As of 2003 when the Reporters Committee for Freedom of the Press last surveyed the state of the law, only 13 states had passed statutes expressly prohibiting the unauthorized installation or use of cameras in private places, and several of those statutes regulate cameras only in certain limited circumstances, such as in locker rooms or restrooms, or where the purpose is to view someone that is partially or fully nude.[25] One federal law, the Video Voyeurism Prevention Act of 2004,[26] similarly restricts only secret videotaping of persons in a state of undress, and only applies in the special maritime and territorial jurisdiction of the United States rather than applying generally. In the face of a 21st century landscape literally littered with cameras that are vulnerable to abuse, this kind of patchwork response to a growing national problem is increasingly unacceptable.

## V. CONCLUSION

In conclusion, Mr. Chairman: the Committee asked us whether Title III needs to be updated in light of the risk of video laptop surveillance. EFF's answer is plainly yes. Congress should—indeed, must—update Title III to protect against unconsented video surveillance in private places at least as strongly as it protects against unconsented eavesdropping on private

[25] See the Reporters Committee for Freedom of the Press, *The First Amendment Handbook, Surreptitous Recording: State Hidden Camera Statutes*, 2003, available at http://www.rcfp.org/handbook/c03p02.html (collecting and describing statutes).
[26] Codified at 18 U.S.C. § 1801.

conversations. Such a change to the law would codify overwhelming Circuit precedent by clearly requiring the government to obtain a court order under Title III's procedures before engaging in secret video surveillance of private places, while also providing civil and criminal liability for warrantless video surveillance, whether by stalkers, computer criminals, employers, schools, or anyone else.

Thank you again, Mr. Chairman, and thanks to the Robbins' family, for shining a spotlight on the need for better regulation in this area. EFF looks forward to the possibility of working with this Committee to update Title III to regulate video surveillance in a manner that appropriately balances the interests of privacy, free expression, and public safety, and I will be delighted to take any questions you may have.

United States Senate
Committee on the Judiciary
Subcommittee on Crime and Drugs

Field Hearing on

VIDEO LAPTOP SURVEILLANCE: DOES TITLE III NEED TO BE UPDATED

Philadelphia, PA
March 29, 2010

Statement of Fred H. Cate
Distinguished Professor and C. Ben Dutton Professor of Law
Indiana University Maurer School of Law
Director, IU Center for Applied Cybersecurity Research

Chairman Specter, Senator Graham, and Members of the Subcommittee,

My name is Fred Cate, and I am a Distinguished Professor and C. Ben Dutton Professor of Law at the Indiana University Maurer School of Law, and the director of Indiana University's Center for Applied Cybersecurity Research, a National Center of Academic Excellence in Information Assurance Education and in Information Assurance Research.

For the past 20 years I have had the privilege of researching and teaching about a variety of privacy, security, and other information law and policy issues. I served as a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information, and counsel to the Department of Defense Technology and Privacy Advisory Committee.

In addition to my academic appointment, I am also a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP, a member of Microsoft's Trustworthy Computing Academic Advisory Board, and editor of the Privacy Department of the IEEE's (Institute of Electrical and Electronic Engineers) *Security & Privacy*, among other activities.

I am testifying today on my own behalf; the views I express should not be attributed to any organization with which I am affiliated.

Chairman Specter, I want to begin by thanking for your leadership in holding this important hearing today, and for inviting me to participate.

The facts concerning Lower Merion School District's provision of laptops to students in Harrington High School and its use of the technological capability to remotely activate the cameras in those laptops are both disputed and the subject of pending litigation, so I will focus instead on some of the broader issues that the provision of remotely accessible cameras on laptops provided to students raise. I would like to make three points:

1. Title III of the Omnibus Crime Control and Safe Streets Act of 1967[1]—the "Wiretap Act" and the subject of today's hearing—needs to be updated to cover video surveillance.

2. The conduct giving rise to today's hearing is only the most recent in a series of examples demonstrating how disconnected today's surveillance technologies have become from the law that purports to regulate them. A revision of federal surveillance law is necessary to address these challenges.

3. There are important steps that institutional providers/users of those technologies can and should take, irrespective of specific legal obligations, to diminish their impact on privacy and other protected civil liberties.

1. Title III and Video Surveillance

The Wiretap Act governs the interception of "wire communications," "oral communications," and "electronic communications."[2] To fit within the definition of "wire communications," the interception must include an "aural transfer," which the statute defines to mean that the human voice must be present at some point during the communication.[3] The definition of "oral communications" requires that the communication intercepted have been "uttered by a person."[4] "Electronic communications" is defined broadly to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," other than a "wire" or "oral" communication.[5]

There has been no suggestion that the remotely activated camera in the case giving rise to this hearing captured anything other than still images, so this conduct would not fit within the definition of a "wire" or "oral" communication." The situation would be different if the camera had been alleged to have captured video accompanied by sound. The capturing of still images unaccompanied by sound might appear to fit within the definition of "electronic communications," but the information captured was not electronic at the time it was captured. As Professor Orin Kerr has written, "[a] still image taken by a camera does not intercept something that has been 'transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system.'"[6]

The reality that the Wiretap Act does not extend to video or other optical surveillance if sounds are not captured at the same time has been highlighted in prior cases in which hidden cameras were installed in bedrooms, bathrooms, changing rooms, and elsewhere causing some states to enact "video voyeurism" laws.[7] Moreover, it is ironic that under the much weaker Foreign Intelligence Surveillance

---

[1] Pub. L. No. 90-351 (codified at 18 U.S.C. §§ 2510-2520).

[2] 18 U.S.C. § 2511(1).

[3] Id. §§ 2510(1), 2510(18).

[4] Id. § 2510(2).

[5] Id. § 2510(12).

[6] Orin Kerr, Response to Phanatic, A Few Thoughts on Robbins v. Lower Merion School District, The Volokh Conspiracy (Feb. 18, 2010) (quoting 18 U.S.C. § 2510(12), available at http://volokh.com/2010/02/18/a-few-thoughts-on-robbins-v-lower-merion-school-district/).

[7] Clay Calvert & Justin Brown, "Video Voyeurism, Privacy, and the Internet: Exposing Peeping Toms in Cyberspace," 18 *Cardozo Arts & Entertainment Law Journal* 469 (2000).

Act of 1978,[8] the gap would not exist if the surveillance were for the purpose of gathering foreign intelligence. As Professor Dan Solove has noted, "[f]oreign agents therefore receive protection against silent video surveillance whereas United States citizens do not."[9]

To avoid this gap in the future it will be necessary to amend the Wiretap Act to apply to visual surveillance as well as auditory surveillance. But doing so will not be a simple as it may seem, because the Wiretap Act deals with intercepting communications between parties, and not the observation of a person or setting. Moreover, the Act does not impose liability if any one party to a communication consents,[10] unless the interception is for the purpose of committing a criminal or tortuous act.[11] It will be critical not to make the amendment so broad that it covers security cameras in public places.

One possibility would be to adopt an amendment mirroring the language concerning "oral communications"—an oral communication "uttered by a person exhibiting an expectation that such communication is not subject to interception subject to interception under circumstances justifying such expectation"[12]—but applying it to "the capturing of still or moving images of a person in a setting in which the individual does not expect to have his or her image recoded and under circumstances justifying such expectation." The offense could be limited to action committed "intentionally," as is the case with the rest of the Wiretap Act, and it could be limited to specific settings, such as the home, if Congress thought necessary.

A fully developed resolution of the issues presented by this gap in federal law is beyond the scope of this testimony. What is clear is that the gap needs to be closed so that federal protection against the secret collection of pictures and videos does not depend on the happenstance of whether sounds are collected at the same time.

2. Surveillance Technology and the Law

The alleged use of a laptop camera to capture images of a student within his home is only the most recent in a long series of events in which modern digital technologies have been deployed in ways that challenge both existing laws and privacy norms. Consider these examples:

- Radio Frequency Identification ("RFID") tags—small computer chips that contain limited information, usually a unique identification number—are used today in pets (and on occasion people) to facilitate identification and provide medical or other important information. Tags are embedded in consumer goods to help prevent shoplifting and fraudulent returns. Electronic toll payment systems, such as EZ-Pass, I Pass, FastPass, and FasTrak, often rely on RFID tags. Governments are adding them to identification cards and important documents.

- Location sensors, including RFID tags, Global Positing System (GPS) devices, cell phones that (as required by federal law) provide the cell phone service provider—not the user—with precise information about the location of each cell phone, OnStar and other vehicle

[8] Pub L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. § 1801-1811).
[9] Daniel J. Solove, "Electronic Surveillance Law," 72 *George Washington Law Review* 1264, 1280 (2004).
[10] 18 U.S.C. §2511(2)(c).
[11] Id. § 2511(2)(d),
[12] Id. § 2510(2).

assistance services, and Wireless Local Area Network ("WLAN" or "WiFi") connections generate a wealth of information—current and historical—about location, speed of movement, direction, etc. Trucking lines, rental car companies, and other businesses now routinely rely on GPS to locate their vehicles. In August 2007, New York City Public Schools reportedly terminated an employee because the location information generated by his employer-provided cell phone showed he was not at work when he claimed to be.[13] And a Connecticut car rental company earned national fame when it used GPS technology to automatically fine drivers $150 every time they exceeded 79 miles per hour for two minutes or more.[14]

- Digital audio and video surveillance technologies have exploded in cities, on highways, in airports, and in many other settings. Digital cameras offer ultra-high resolution images capable of identifying faces and license plate numbers from hundreds of feet away. They are increasingly wireless, which means they can be installed without expensive wiring and can operate in buses and subways. They are centrally controlled, so that an operator miles away can cause a traffic or security camera to pan, tilt, or zoom in on specific targets. And they are digital, which makes the data they collect easier and cheaper to store, and share, and capable of analyzing with sophisticated voice, face, and threat recognition programs.

- Small digital cameras and cameras in cell phones have proliferated, and with them have come a wide range of uses ranging from monitoring children and in-home employees to capturing images of unsuspecting people in locker rooms, bathrooms, changing rooms, on escalators, carnival rides, public transportation, and other settings.

- Biometric identification, such as fingerprints and retinal and iris scans, are becoming increasingly common to identify students in college cafeterias, employees, even visitors to Walt Disney World must now provide a fingerprint in an effort to prevent sharing of tickets). DNA recognition is not yet widely used, but researchers are working on "sniffers" that will collect DNA from skin cells, even those routinely discarded. When perfected, this technology will allow investigators to determine whether an individual was in a room or vehicle, and when, by analyzing the discarded cells found there.

These are just a few examples of the many ways in which applications of new technologies are challenging our understanding, and the law's protection, of privacy. The Technology and Privacy Advisory Committee ("TAPAC"), a "blue ribbon"[15] bipartisan independent committee appointed by Secretary of Defense Donald Rumsfeld in 2003 to examine privacy and security issues, wrote in 2004 in its final report that "[l]aws regulating the collection and use of information about U.S. persons are often not merely disjointed, but outdated."[16] They "fail to address extraordinary developments in digital technologies, including the Internet," even though those technologies have "greatly increased the government's ability to access data from diverse sources, including commercial and transactional

[13] David Seifman, "'Track' Man Is Sacked—GPS Nails Ed. Guy," *New York Post*, Aug. 31, 2007, at 27.

[14] American Car Rental, Inc. v. Commissioner of Consumer Protection, 273 Conn. 296, 869 A.2d 1198 (2005).

[15] Ronald D. Lee & Paul M. Schwartz, "Beyond the 'War' on Terrorism: Towards the New Intelligence Network," 103 *Michigan Law Review* 1446, 1467 (2005);

[16] U.S. Department of Defense, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 6 (2004).

databases." As a result, "[c]urrent laws are often inadequate to address the new and difficult challenges presented by dramatic developments in information technologies. And that inadequacy will only become more acute as the store of digital data and the ability to search it continue to expand dramatically in the future."[17] "It is time to update the law to respond to new challenges."[18]

Law almost always lags behind technology and society. The Supreme Court initially refused to apply the Fourth Amendment to wiretapping at all, and it took the Court 39 years to reverse that decision.[19] Conversely, in 1934 Congress prohibited wiretapping in any form and for any purpose.[20] It took 34 years before Congress recognized the potential of electronic surveillance, properly regulated, to aid law enforcement, and another twelve before it statutorily authorized its use to advance national security.[21]

Individual courts and states are struggling to figure out how to apply old laws to new challenges. But it is increasingly clear that the thoughtful intervention of Congress is necessary.

Federal surveillance laws, including Title III, are especially affected by technological changes. Those laws today suffer from what Professor Solove has described as "profound complexity."[22] Professor Kerr has written that "the law of electronic surveillance is famously complex, if not entirely impenetrable."[23] Courts agree with these assessments and have described "surveillance law as caught up in a 'fog,' 'convoluted,' 'fraught with trip wires,' and 'confusing and uncertain.'"[24] As you take up your timely and important review of Title III, I encourage you not to ignore other challenges to, and deficiencies in, that law.

3. Independent Steps to Protect Privacy

Finally, there are important independent steps that institutional providers/users of new technologies can—and should—take to protect privacy and other civil liberties, without regard for whether they are legally required to do so. For example, a school district, any school district, considering activating built-in cameras in laptops supplied to students would be well advised to ensure that:

1. They have a written policy in place governing the terms under which cameras will be activated, the use that will be made of any images captured, how long those images will be retained, and under what conditions they will be shared with third parties, including law enforcement.

---

[17] Id.

[18] Id.

[19] Olmstead v. United States, 277 U.S. 438 (1928); United States v. Katz, 389 U.S. 347 (1967).

[20] Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064 (codified as amended at 47 U.S.C. § 605).

[21] Omnibus Crime Control & Safe Streets Act of 1968, Pub. L. 90-351, § 802, 82 Stat. 212 (codified as amended at 18 U.S.C. § 2510-2520); Foreign Intelligence Surveillance Act of 1978, Pub L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801-1811).

[22] Solove, "Electronic Surveillance Law," supra at 1292.

[23] Orin S. Kerr, "Lifting the 'Fog' of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law," 54 *Hastings Law Journal* 805, 820 (2003).

[24] Solove, "Electronic Surveillance Law," supra at 1293.

2. Their policy reflects thoughtful consideration and clear steps to ensure that cameras are not activated in private spaces, such as personal homes, bathrooms, locker rooms, and the like, absent exceptional circumstances which should be enumerated in the policy.

3. They identify in writing which school district officials have the authority to turn on the cameras and to access the resulting images.

4. They provide clear and conspicuous notices to students (and to their families) of the presence of the cameras, the fact that they can be remotely activated, and the district's policy concerning their activation.

5. They restrict access to the codes or other control mechanisms necessary to activate laptop cameras remotely.

6. They provide appropriate training to all employees with access to those codes or other mechanisms.

7. They employ appropriate oversight mechanisms to provide strong incentives for compliance with the relevant district policies (and applicable laws), detect noncompliance speedily if it occurs, and ensure that senior district officials are made aware immediately on any violations. These mechanisms could include audit logs, two-person activation requirements, and routine audits.

8. They build into procurement and other processes an appropriate evaluation mechanisms to ensure that the district is not acquiring surveillance technologies or sensitive personal data without a compelling reason for doing so.

Protecting privacy is the responsibility of all responsible organizations, especially those in the public sector.

Mr. Chairman, thank you again for the opportunity to appear before the subcommittee today. The topic you have raised is an important one in its own right and as part of a growing trend in which new technologies challenge increasingly outdated privacy laws. I urge you and your colleagues to begin the vital process of not only closing gaps in the Wiretap Act, but also of more broadly updating federal privacy law laws for the 21st century.

Biography

Fred H. Cate is a Distinguished Professor, C. Ben Dutton Professor of Law, and Adjunct Professor of Informatics and Computing at Indiana University. He is the founding director of the university's Center for Applied Cybersecurity Research, a National Center of Academic Excellence in Information Assurance Education and in Information Assurance Research. He works at the forefront of privacy, security, and other information law and policy issues.

He is a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP, a member of Microsoft's Trustworthy Computing Academic Advisory Board, the Board of Directors of the Center for Applied Identity Management Research, the Board of Directors of The Privacy Projects, the Board of Advisors of Trustee, and BNA's *Privacy & Security Law Report* Advisory Board. He serves as editor of the Privacy Department of the IEEE's (Institute of Electrical and Electronic Engineers) *Security & Privacy*.

Previously, Professor Cate served as a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information, counsel to the Department of Defense Technology and Privacy Advisory Committee, reporter for the third report of the Markle Task Force on National Security in the Information Age, and a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, and chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities. In 2008 he served as a privacy advisor to the campaign of then-Senator Barack Obama.

Professor Cate has testified before numerous congressional committees, and he speaks frequently before professional, industry, and government groups. He has spoken throughout the United States and in Belgium, Canada, China, Finland, France, Germany, Italy, Japan, Switzerland, Taiwan, Trinidad & Tobago, and the United Kingdom. He is the author of more than 100 articles and books, including *Privacy in the Information Age, The Internet and the First Amendment*, and *Privacy in Perspective*. He appears regularly in national media.

Professor Cate is the President and a Fellow of the Phi Beta Kappa Society and an elected member of the American Law Institute. He attended Oxford University and received his J.D. and his A.B. with Honors and Distinction from Stanford University. He is listed in *Who's Who in the World, Who's Who in America, Who's Who in American Law*, and *Who's Who in American Education*. *Computerworld* listed him in its two most recent rankings of "Best Privacy Advisers."

STATEMENT OF JOHN LIVINGSTON, CEO OF ABSOLUTE SOFTWARE
BEFORE THE SUBCOMMITTEE ON CRIME AND DRUGS
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
PHILADELPHIA, PENNSYLVANIA
MARCH 29, 2010

Chairman Specter, Members of the Subcommittee, Absolute Software is pleased to have this opportunity to discuss with the subcommittee Absolute's products and services, as well as our protocols and policies as they relate to privacy issues, which is something that Absolute values and cares deeply about.

I co-founded Absolute Software in 1994 with the notion that individuals and businesses should be able to manage, secure and recover their mobile devices regardless of their physical location. Since that time, Absolute has developed one of the premier managed theft recovery services in the world. Our security-as-a-service solutions protect more than 5 million computers worldwide with subscribers who range from individuals to the largest public and private sector organizations. To date, we have recovered over 13,500 computers in 50 different countries with our flagship product suite, Computrace. We average approximately 100 stolen computer recoveries each week.

Absolute believes very strongly in protecting computer theft victims and mitigating the multiple downstream consequences of computer theft. For an organization with a lost or stolen computer, the cost of the hardware is really just the beginning. In addition to lost productivity and competitive threats, an organization that experiences a data breach may be subject to fines, media scrutiny, and a damaged reputation. Computer theft has other costs and consequences including the potential theft of personal identifying information that may later be sold or otherwise misused by identity thieves.

In fact, we have assisted the Philadelphia police on many occasions, including cases where recovering the laptop led to apprehending a child pornographer or recovering illegal drugs, weapons, and stolen cash. This is not atypical. Our case experience indicates that laptop thieves are often involved with other very serious crimes, including child pornography, drug trafficking, large scale burglaries, including involving public school districts.

- We assisted the San Diego School District in recovering 13 laptops that had been stolen during a breaking and entering. The thieves were also charged with possession of methamphetamines and various parole violations.
- Computrace uncovered a Southwest Airlines luggage handler theft ring at O'Hare Airport, after which law enforcement arrested 5 workers, recovered 8 laptops, 4 cameras, 2 GPS units, and cash.
- In Florida, our technology helped to capture a career criminal who had been burglarizing offices and taking 12-15 laptops at a time. He was sentenced to ten years in prison for his various crimes.

- Working with information provided by Absolute, police were able to identify an unauthorized user on a stolen laptop and recovered drugs, handguns, and hundreds of stolen social security and credit card numbers from his residence. The value of the stolen credit card information alone was estimated at $300,000.

We believe that in significant part these successes are possible because our post-theft recovery services are carried out by Absolute's trained theft recovery personnel. The theft recovery process only begins when the customer reports their computer as stolen to local law enforcement. Then the customer must report the theft to Absolute, provide the police report file number (which is required before any theft recovery process begins), and their authorization to have Absolute's Theft Recovery team start the investigation. Our trained Computrace investigative team of law enforcement veterans coordinates the entire theft recovery process and partners directly with local law enforcement. We are ISO 27001 certified and have policies, procedures, and controls to protect customer data, which I would be happy to describe if that is of interest to your Committee.

Thus, our Computrace solution is premised upon a managed theft recovery model that relies upon filed police reports to open a case investigation, which is then handled by our staff of highly trained former law enforcement personnel. Some of our competitors instead offer end-user oriented solutions, similar to the LANRev "Theft Track" tools that a purchaser (such as an IT Administrator at a school district) could choose to activate to enable taking still images from a laptop's webcam. Absolute did not itself develop or offer camera functionality in its product line, because we did not see a need for such a tool in our very different, and in our view superior, managed recovery model. We acquired LANRev's assets late last year for their computer inventory and asset management functionality, and, through a software patch offered to the Theft Track customers we acquired, disabled the webcam feature earlier this year.

With that, I conclude my comments, and welcome your questions, Senator.

**Statement of**

**Robert Richardson**
**Director, Computer Security Institute**
**Robert.Richardson@ubm.com**

**Before the**
**United States Senate**
**Committee on the Judiciary**
**Subcommittee on Crime and Drugs**

Chairman Specter, Ranking Member Graham and members of the Crime and Drugs Subcommittee, thank you for inviting my written statement and for this opportunity to speak to the issue of video surveillance, particularly as it relates to surveillance using common consumer mobile computing devices such as notebooks, cell phones, and personal digital assistants. These devices, because of their ubiquity, clearly present opportunities for enhanced communication, but they also challenge our notions of security practices as they relate to privacy and surveillance. As Director of the Computer Security Institute, I am engaged daily with these issues as they relate to organizations that maintain large computer and network infrastructures.

The instigation for our discussion today was the desire of one such organization to protect its computer assets. As one would probably expect, concern that mobile assets may be lost or stolen is completely well founded.

One project undertaken by the Computer Security Institute over the past fourteen years is an annual survey of our information security professional community, specifically within the United States. In the most recent survey, 42% of 443 respondents said that their organizations had suffered the theft of laptops or mobile devices in the previous year. Only infection by malicious software, or *malware*, reported by 64% of respondents, was more prevalent.

Perhaps ironically, the modus operandi of today's sophisticated malware is not at all unlike that of the software deployed by some organizations to monitor their notebook computer assets. Both with tracking software and malware, a fundamental level of direct control of the device is transferred to a third party at a distance. This transfer is achieved in both cases because both malware and tracking software have gained or been granted access to the most extensive level of control of the computer, so-called "root" control. Most issues of privacy and access within the confines of a computer have, at their root, the issue of root access.

When the owner and the primary user of a device are one and the same, control and responsibility is easily understood and it is the user who has control of the root account. But in the instance of, say, an employer that loans a notebook to an employee, the employer may well withhold root privileges from the employee. This gives the employer more control over the device than the user, and indeed more control than the user may be aware of, such as the ability to remotely operate a built-in camera.

Root control may be abused in many ways, including by surreptitious spying. But this notion of root control is a necessary one and, extended only slightly, gives us an opening to separate and

protect different categories of use within a device. There can be a category of "workplace" use, for example, that is entirely walled off from "personal" use.

There are multiple ways to achieve this that it would be too lengthy and technical a discussion to delve into here, but in fact most Americans are already familiar with one such division of control. Ninety-five percent of cell phones sold each year within the US are "locked" phones, meaning that their use is controlled and restricted by the carrier that originally sold the phone and that is providing service to it. Using the phone for conversation or texting is understood to be a context where the user is in control. That same user, however, cannot update the core software that runs the phone. The service provider can and does because the service provider has what is in effect root control of the phone.

It is possible, in short, to "lock down" part of a system so that the locked down elements function as a complete computer system unto themselves, with separate software applications and separate storage for files. That this locked down environment is truly separate from the rest of the computer can be rigorously demonstrated using well understood techniques based on advanced forms of encryption as well as a computing framework known as "trusted computing."

Almost all notebook computers sold since 2004 include a Trusted Platform Module housed in a sealed, tamper-proof component within the computer. This provides a reliable foundation for a protected, high-control partition of the computer. In the vast majority of cases, however, this TPM functionality is not enabled and it would be disingenuous not to note that trusted computer systems have raised a great deal of controversy within the information security

community. This controversy, however, stems precisely from a fear that third parties such as Microsoft will have overreaching control over consumer-owned PC's. This is not of concern when we are speaking of an organizational owner extending control over its own PCs.

Within this locked down system, a third party such as a school or employer has an oasis of control. If they don't want to allow chat programs, chat programs can be barred. If they don't want pornography stored, they can scan for it and monitor employee use at will. And the user of that system will know that whenever they are using this system in this workplace context, they may well be monitored.

On the same system, however, it is possible to use what effectively is a second computer that is not locked down, or that is locked down in a less restrictive way. That we can create clear technical boundaries means that we can, by extension, create clear legal boundaries.

We have the option to legislate in a way that recognizes the possibility of such boundaries. By doing so, we can establish that the context in which any kind of surveillance occurs is either clearly within or outside of legal bounds. I appreciate the opportunity to discuss this important issue and will be happy to answer any questions from the Subcommittee.

**Statement of Marc J. Zwillinger**

**Partner**

**Zwillinger Genetski LLP**

**before the**

**U.S. Senate Committee on the Judiciary**

**Subcommittee on Crime and Drugs**

**for the hearing on**

**Video Laptop Surveillance: Does Title III Need to Be Updated?**

**March 29, 2010**

I am pleased to appear before the Subcommittee to testify about the possibilities of amending Title III of the Omnibus Safe Streets Act of 1968 to include photographic and video surveillance. By way of background, I am a former federal prosecutor from the United States Department of Justice Computer Crime and Intellectual Property Section, and have been representing companies, including Internet Service Providers and Social Networking Companies, on issues related to electronic surveillance and the Electronic Communications Privacy Act for the last ten years. As part of that work, I have litigated surveillance-related issues in several district and appellate courts. I also teach a course in cybercrime law as an adjunct professor at the Georgetown University Law Center in Washington, DC. I am testifying today solely in my individual capacity as a practitioner and a law professor and not on behalf of any clients.

Every so often, an incident like what happened in the Lower Merion School District comes to the public's attention, spurring inquiries into whether undisclosed video or photographic surveillance is a violation of Title III, and, if not, whether Title III should be amended to cover such conduct. Recently, a similar discussion took place about the hotel room peephole videos of ESPN reporter Erin Andrews, which were created by a man later convicted of stalking Andrews. A review of similar press reports and civil and criminal cases from the past five years reveals numerous incidents of potential abuse of surveillance technology to photograph or create videos of people in places that a reasonable person would expect to be free from video surveillance. Many of these examples are especially disturbing because the surveillance targeted children. These examples include:

- January 2010 – Islesford, ME. A man was sentenced for secretly videotaping his girlfriend's underage daughter when she was undressing.
- December 2009 – Easton , PA. A lawsuit was filed against Wal-Mart and employees were terminated after a video camera was found to be installed in a unisex bathroom.
- April 2009 – Morgantown, WV. Two law enforcement officers were sued for using a mall surveillance camera to watch girls trying on dresses at a local mall.
- May 2007 – Gig Harbor, WA. Images captured by surveillance cameras at school were used to show parents a same-sex display of affection witnessed on school grounds.
- March 2007 – Atlantic City, NJ. Casino employees were suspended for using casino surveillance cameras to focus on the breasts of women in the

casino. Similarly, it appears that Caesars Atlantic City Hotel Casino was previously fined for the same misconduct.

- August 2005 – Newark, NY. A Police Department employee resigned after being arrested on a charge of using a shoe camera to spy on a teenage girl in a dressing room.
- April 2005 – San Francisco, CA. A police officer was suspended for allegedly using a surveillance camera to ogle women at San Francisco Airport.
- August 2004 – Ithaca, NY. A landlord was charged under NY state law for illegal surveillance of woman in rental properties.
- July 2003 – Overton County, TN. Overton County parents filed suit, charging that school officials allowed surveillance cameras to be installed and then failed to secure the images. The cameras reportedly captured students, ages 10-14, in various stages of undress in locker rooms.
- July 2003 – Atlanta, GA. A woman sued Toys R Us after noticing a hidden video camera in a hole in the ceiling in the bathroom.
- September 2002 – OH. A man filed a lawsuit against Marriott hotel after finding a hidden camera in a light fixture in his hotel room.
- March 2002 – Nashville, TN. 14 Nashville Kat cheerleaders filed suit against the arena's management company and two of its former employees for installing hidden cameras found in their dressing area; and
- In the case that led to the 7th Circuit's ruling in *Doe v. GTE*,[1] athletes at Northwestern University were secretly videotaped in locker rooms and copies of the video were sold.

Title III currently does not address these problems. It is fairly well-settled that silent video surveillance is outside the scope of the statute. Though these and other examples of surveillance-related misconduct make it tempting to conclude that Title III should be amended to prohibit this type of behavior, doing so may be a mistake. While we are now horrified by the idea that remote video or photographic surveillance of our children in private places is possible without our consent, at other times we are comforted by the notion that video surveillance helps keep our children safe. From the surveillance cameras that help us protect children at places like Hershey Park or Sesame Place, to the closed-circuit TV cameras outside homes and apartments, and even to the nanny-cams that some parents install above cribs to be sure their babies are not injured by their caretakers, parents often rely on silent video surveillance to be an extra pair of eyes when they cannot be in several places at the same time. Similarly,

[1] 347 F.3d 655 (7th Cir. 2003).

companies rely on such surveillance to protect their employees and their property. Thus, when considering how to address the inappropriate use of video surveillance technology, we also need to consider the beneficial uses of such technology to determine whether allowing such surveillance in certain places strikes the right balance between privacy and security.

In thinking about amending a comprehensive regime like Title III, it is important to keep in mind the different purposes that the statute serves. First, it sets out the standards by which law enforcement must conduct certain types of surveillance operations. Second, it provides a criminal cause of action so the government can punish those who violate the provisions of the statute. Third, it provides a civil cause of action for aggrieved parties to recover damages from someone whose violation of the statute has injured them. It does so by making it illegal to intentionally intercept, endeavor to intercept, or procure any other person to intercept, any wire, oral, or electronic communication.

Title III broadly defines both "wire communications" and "electronic communications.". Wire communications are those communications involving the human voice, like phone calls, and electronic communications that include any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system, like emails. Only the definition of oral communications is limited by the inclusion of a clause restricting the type of person-to-person communication it covers to those uttered by a person "exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." 18 U.S.C. § 2510(2). Thus, while Title III prohibits the interception of any wire or electronic communications, the statute only protects those spoken communications where the speaker has a reasonable expectation that the communication will not be intercepted.

In analyzing the effect of amending Title III to prohibit video or photographic surveillance, we must first consider how such prohibitions would fit within the statute. If video or photographic surveillance was covered in the same manner as wire or electronic communications – without consideration of whether a reasonable expectation of privacy existed– there would be two immediate effects. First, it would likely make illegal the array of public and private remote surveillance and security cameras that can be found today at every ATM, gas station, casino, doorstep, and light pole that are used for a multitude of legitimate purposes including security, crime fighting, traffic analysis, and scientific

observation. Second, it could turn well-intentioned journalists, security professionals, parents, and scientists into serious criminals. In a worst-case scenario, a court might interpret the statute to make it illegal to take a picture without the subject's consent. Beyond problems with enforcement, such a prohibition may not be constitutional in light of the First Amendment.[2]

To avoid these consequences, video surveillance would have to be treated like oral communications and only prohibited in cases where the person captured on video had a reasonable expectation of privacy. Even still, when viewed in light of the three functional purposes of Title III, adding video may create more problems than it would solve. First, as to the government's use of surveillance for fighting crime, any privacy protection benefits would be marginal. The majority of Courts of Appeal have held that video surveillance by the government in an area where an individual has a reasonable expectation of privacy implicates the Fourth Amendment, and many circuits have also held that search warrants for video surveillance must meet certain higher, constitutional standards, like those required under the Fourth Amendment.[3]

Even assuming that adding video surveillance to the types of interceptions the Wiretap Act prohibits would provide some privacy enhancements *vis-a-vis* law enforcement's use of surveillance, the increased uncertainty it would create as to what would now constitute a crime or lead to civil liability would likely outweigh any such benefit. Currently, for oral communications, the standard for "exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation," 18 U.S.C. § 2510(2), roughly mirrors the standard under the Fourth Amendment, which must be determined on a case-by-case basis, and is highly fact-dependent. As a result, certain legitimate types of security video surveillance acceptable for safety reasons would be called into question if it could be argued that the video was taken in a public or quasi-public space where a reasonable expectation of privacy existed. As a result, these uses would likely be chilled.

---

[2] *See, e.g., Gilles v. Davis*, 427 F.3d 197, 212 n.14 (3d Cir. 2005); *Smith v. City of Cumming*, 212 F.3d 1332, 1333 (11th Cir. 2000) (First Amendment right to film police conduct); *Blackston v. Alabama*, 30 F.3d 117, 120 (11th Cir. 1994) (finding that plaintiffs' interest in filming public meetings is protected by the First Amendment); *Fordyce v. City of Seattle*, 55 F.3d 436, 439 (9th Cir. 1995) (recognizing a "First Amendment right to film matters of public interest").

[3] *See, e.g., United States v. Falls*, 34 F.3d 674 (8th Cir. 1994); *United States v. Koyomejian*, 970 F.2d 536 (9th Cir. 1992); *United States v. Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990); *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987); *United States v. Biasucci*, 786 F.2d 504 (2d Cir. 1986); *United States v. Torres*, 751 F.2d 875 (7th Cir. 1984).

Under existing Title III case law addressing oral communications, distinguishing between situations where it is acceptable to record audio communications and where it is not is difficult. Federal and state cases have questioned the acceptability of recording oral communications without the participants' knowledge in many different situations, including: employers recording employees' conversations in a U.S. post office workspace;[4] near a traffic reporter's work station;[5] in security personnel locker areas;[6] in hotel hallways with no other guests around;[7] and in college fraternity houses.[8] What those cases teach is that the answer is mostly "it depends." It depends on a wide variety of factors including the nature of the physical location, the participants' actions, the potential for third-parties to be present, the need for technological enhancements to intercept the communications, and more.[9] Applying this case law to the video surveillance context would create substantial uncertainty, as even fewer courts have needed to confront the questions of the legality of private audio recordings in semi-private places, where someone may not have an expectation of privacy under the Fourth Amendment to the constitution, but where they have a subjective and an objective expectation that their communications will not be intercepted. These places may include private booths at restaurants, elevators with no other passengers, or even in a locked ATM section of a bank with no other patrons, because only silent video surveillance is used regularly in such settings. But if Title III were revised to include video, every wrongdoer who was caught on a security camera in any of these areas could challenge that surveillance as a possible violation of Title III. Therefore, well-meaning parents, employers, and even journalists would need legal advice before setting up cameras – even if they were designed to enhance their safety or for news reporting – or risk potential civil liability and criminal punishment.

There are pro-privacy alternatives to amending Title III that would seem to address the concerns raised by the Lower Merion and Erin Andrews cases without resulting in diminished security or a spate of new litigation. Generally, the events

---

[4] Walker v. Darby, 911 F.2d 1573 (11th Cir. 1990).

[5] *Wesley v. WISN Division-Hearst Corp.*, 806 F. Supp. 812 (E.D. Wis. 1992) (radio station employee sued employer for activating microphone in radio station to record her conversation with a co-worker).

[6] *Thompson v. Johnson County Cmty. Coll.*, 930 F. Supp. 501 (D. Kan. 1996) (community college security personnel sued college for silent video surveillance in area where storage lockers were used by security personnel)

[7] *Pennsylvania v. Wright*, No. 2318 Crim. 1993, 1994 WL 897168 (Pa. Ct. C.P., Cumberland County July 12, 1994).

[8] *Iowa Beta Chapter of Phi Delta Theta Fraternity v. Univ. of Iowa*, 763 N.W.2d 250 (Iowa 2009) (fraternity sued state university for recording conversations in fraternity meeting room).

[9] *See, e.g., Kee v. Rowlett*, 247 F.3d 206 (5th Cir. 2001) (explaining the 6 primary factors used by courts in evaluating privacy claims related to interceptions of oral communications, and noting others).

that most concern us involve either: (a) video surveillance of minors; (b) surveillance conducted in an area where someone would be reasonably likely to disrobe; or (c) surveillance tools that are implemented for lawful purposes but used improperly, usually for voyeuristic purposes. Legislation to prevent these types of harms – at least on federal land – was enacted in 2004 under the name the "Video Voyeurism Prevention Act." This statute prohibits the disturbing types of privacy intrusions described above without prohibiting the legitimate use of silent video surveillance as a security measure.

Under the Video Voyeurism Prevention Act, it is a federal crime to "capture an image of a private area of an individual without their consent" if the person "knowingly does so under circumstances in which the individual has a reasonable expectation of privacy." 18 U.S.C. § 1801(a). For purposes of this statute, "reasonable expectation privacy" is specifically defined to cover "circumstances in which a reasonable person would believe that he or she could disrobe in privacy, " *id.* § 1801(b)(5)(A), or "circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether the person is in a public or private place," *id.* § 1801 (b)(5)(B), thus avoiding the fact-intensive constitutional test. Thus, someone who photographed or videotaped an individual in a hotel room, locker room, or bedroom with the intent to capture their private areas would be covered. While this approach is not perfect –it does not cover, for example, the remote activation of a camera that is not done for a voyeuristic purpose – it could provide a better starting point than Title III to build a nationwide statute that prohibits videotaping an individual in an area where he or she could reasonably expect to disrobe, whether or not it was done with voyeuristic intent.

Some states have also attempted to address this problem by drafting nuanced legislation that targets inappropriate voyeuristic behavior and surveillance that intrudes into private spaces, like bedrooms and bathrooms, without necessarily restricting the ability of parents, employers and property owners to use silent video surveillance for safety. For example, Delaware makes it a crime to capture without consent the image of another person who is getting dressed or undressed in any place where persons normally disrobe, including but not limited, to a fitting room, dressing room, locker room, or bathroom, where there is a reasonable expectation of privacy. The statute contains an exemption for parents filming their own children except if they are doing it for impermissible purposes. *See* Del. Code Ann. tit. 11, § 1335(a)(6) (2010).

Other states take a different approach. Georgia, for example, bans the photographing or recording of any activities occurring in any private place and out of public view; but creates exemptions allowing owners of real property to use video to observe, photograph, or record the activities of persons who are on the property or approaching it in areas where there is no reasonable expectation of privacy for security purposes, crime prevention, or crime detection.

These state statutes could serve as a model for future federal legislation. The key deficiency in these approaches, however, is that neither of the statutes mentioned properly restricts the type of behavior that results when the operators of legitimately-placed surveillance equipment use the technology for illicit purposes. The key to preventing such circumstances may be to ensure that any use of remotely controllable silent video surveillance (where the cameras are not in fixed positions or always on) is accompanied by strict internal controls as to when the technology can be activated and/or refocused and for what purposes. To the extent any federal legislation is proposed in this area, one solution is to condition a safe harbor from vicarious liability on the implementation of written and comprehensive control procedures designed to prevent against inappropriate use of technology. That would reinforce the idea that when companies or governments are in control of private images related to third-parties, they should be able to demonstrate that they have taken reasonable efforts to prevent inappropriate access to or disclosure of those images.

The idea that we, or our children, could be subject to video surveillance in areas that we believe to be private is troubling. What really bothers us about silent video surveillance is the fact that the camera may catch us unaware and possibly undressed. In the hierarchy of privacy protection, however, we should be more focused on ensuring that our private thoughts, conversations, phone calls, emails, instant messages and text messages remain sacrosanct and that neither the government nor private individuals can intercept them or retrieve them from third parties without adequate notice or probable cause to believe that we are committing a crime. There is no question in my mind that our Electronic Communication Privacy statutes are in need of broad reform, especially to bring the privacy protections for stored communications into the modern age of social networks and cloud computing. When addressing video surveillance, however, we need to carefully craft specific legislation to target the specific harms we want to prevent without eliminating the ability of government and

private citizens to conduct legitimate video surveillance for safety and security purposes.

Thank you for the opportunity to testify today. I would be pleased to work with the Subcommittee to craft legislation to accomplish those goals.



VerDate Nov 24 2008 10:16 Sep 28, 2010 Jkt 058268 PO 00000 Frm 00065 Fmt 6633 Sfmt 6011 S:\GPO\HEARINGS\58268.TXT SJUD1 PsN: CMORC

58268.034