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

## 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=oLB4LNFvbFI.

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.