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."