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.