2015

Digital Peepholes | Remote Activation of Webcams: Technology, Law and Policy

Lori Andrews

DIGITAL PEEPHOLES

REMOTE ACTIVATION OF WEBCAMS: TECHNOLOGY, LAW, AND POLICY

By Lori Andrews, JD, Michael Holloway, JD, and Dan Massoglia, JD

• Institute for Science, Law and Technology, IIT Chicago-Kent College of Law •

DIGITAL PEEPHOLES

REMOTE ACTIVATION OF WEBCAMS: TECHNOLOGY, LAW, AND POLICY

Lori Andrews, JD, Michael Holloway, JD, and Dan Massoglia, JD

THE INSTITUTE FOR SCIENCE, LAW & TECHNOLOGY, a not-for-profit, cross-disciplinary collaborative effort at the Illinois Institute of Technology, trains leaders and provides in-depth, thoroughly-researched answers to the toughest issues that arise at the edges of science and law.

The *Digital Peepholes* project is part of the Chicago-Kent Privacy program at IIT Chicago-Kent College of Law. CK Privacy provides an opportunity for students, faculty members, policymakers and the public to assess the ways in which technologies present new challenges to privacy and data protection, as well as to develop technical and legal ways to better ensure privacy and improve data protection.

http://www.ckprivacy.org

Layout and design by Daniel Saunders
IIT Chicago-Kent Faculty Marketing Coordinator

CONTENTS

EXECUTIVE SUMMARY

The remote activation of webcams raises serious privacy concerns that existing laws do not adequately address. Webcams have transformed entertainment, medicine, home security, and many other fields. But they have also been used to spy on people in shocking ways. Currently, webcams can be remotely activated by governments, businesses, or hobbyist hackers known as "ratters," each with a distinct set of goals, but all of whom commit egregious invasions of privacy through remote activation. Hundreds of thousands of people have been the targets of surreptitious remote webcam activation, yet there has been no meaningful legislative response to the problem. Strong legal prohibitions are needed to prevent invasions of privacy by remote webcam activation.

The Constitution guarantees privacy and freedom against unreasonable searches and seizures by the government. These guarantees should preclude the government from remotely activating webcams, given that webcams are frequently located in the home, where privacy rights are at their strongest. Yet because the existing laws on government electronic surveillance allow secret proceedings and provide few opportunities for public oversight, there is no way of knowing how many times remote webcam activation has been approved by a judge, or been used without any judicial authorization. The FBI has the technological ability to activate a webcam without triggering the light meant to notify the user; yet we have no information on how many times the FBI has done so. Given the grave constitutional infirmities of remote webcam activation and the presence of less invasive alternatives, laws are needed to prevent the government from remotely activating webcams.

Businesses have engaged in shocking abuses of remote webcam activation technology. Rent-to-own stores have installed remote webcam activation capabilities on rental computers and used it to spy on their customers. Other companies sell remote access software that they activate when a computer is reported stolen, attempting to gather information on the purported thief to hand to the police. Both of these practices have led to egregious privacy violations of innocent people. Yet because of a minimum damages requirement in the federal Computer Fraud and Abuse Act and outdated language in the Electronic Communications Privacy Act, victims of webcam spying have little recourse under federal law. Shockingly, people who have

their webcams surreptitiously activated and were spied on have been held to have no recourse under the federal unauthorized access and wiretap laws.

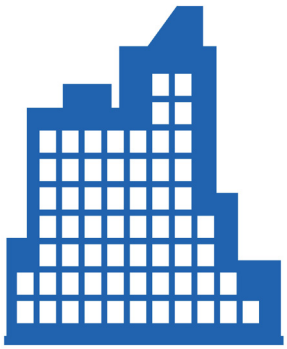
Taking advantage of cheap and user-friendly remote access software available in the murkier corners of the internet, individual "ratters" are able to take control of victims' computers and remotely activate their webcams. Ratters, often young men, activate the webcams of their victims, often young women, and attempt to capture photos of them nude or having sex. They can then extort their victims—"slave girls," as they are often dubbed in ratter circles—for additional nude photos. They trade or even sell copies of the private images to others in their online circles. Ratters have victimized thousands of young women, including minors. While there have been successful prosecutions of prominent ratters, there is no law specifically addressing the problem of remote webcam activation.

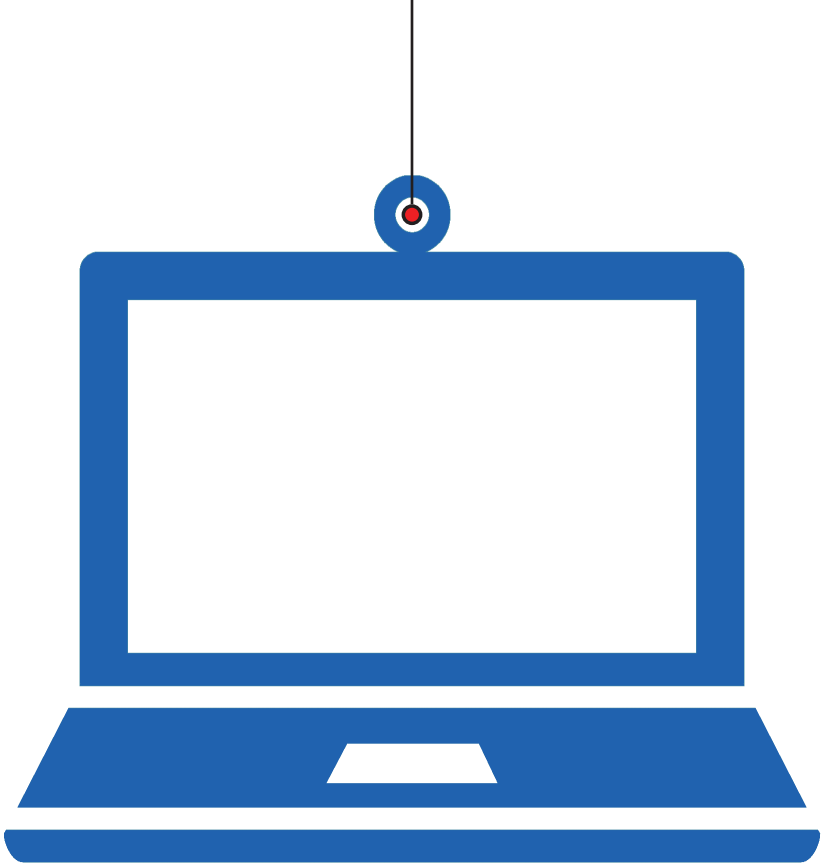
Each of these situations demands action to prevent invasions of privacy through remote webcam activation. Given its questionable effectiveness and high level of intrusiveness, remotely activating webcams should be clearly prohibited as a law enforcement investigative technique, and the rules of criminal procedure should not be modified to encourage its uses. Private businesses should similarly be banned from employing remote webcam activation, as its supposed benefits for theft prevention and recovery do not justify the flagrant violations of privacy that inevitably occur when the technology is activated. Furthermore, federal and state law should be updated to provide a civil remedy for victims of surreptitious webcam spying. Finally, law enforcement and the judicial system should make greater efforts to prevent surreptitious webcam activation and to investigate and punish anyone who uses a webcam to violate a computer user's privacy.

We need stronger laws and regulations to protect our right to privacy as we move forward into the interconnected age.

WEBCAMS

CAN BE REMOTELY ACTIVATED BY GOVERNMENTS, BUSINESSES, OR HOBBYIST "RATTERS," ALL OF WHOM COMMIT EGREGIOUS INVASIONS OF PRIVACY THROUGH REMOTE ACTIVATION.





1. INTRODUCTION

Webcams have transformed contemporary life. Webcams are used for numerous purposes, including participating in video calls with friends and family worldwide;[1] preventing theft and providing home security;[2] monitoring babies[3] and family members in nursing homes to ensure their well-being;[4] providing medical care and advice;[5] live streaming events;[6] and enabling website logins with facial recognition.[7] Webcams also provide entertainment: over 100 hours of video, much of it produced by webcam, are uploaded to YouTube each minute,[8] and webcam feeds featuring cute animals are promoted as "ambient entertainment" by television networks like Animal Planet.[9] The chief minister of the Indian state of Kerala even installed a live-streaming webcam in his office as an anti-corruption measure.[10]

While webcams provide valuable functions for many internet users, they also raise serious privacy concerns. Readily available remote administration tools allow third parties to gain unauthorized access to users' computers and activate their webcams, often without their knowledge. Governments around the world use powerful spyware to gain control over individuals' computers, including the ability to covertly activate the webcam, and in some cases use it to target dissidents.[11] The Federal Bureau of Investigation (FBI) has the ability to remotely activate a webcam without

detection[12] and has gone to court to request a warrant to do so.[13]

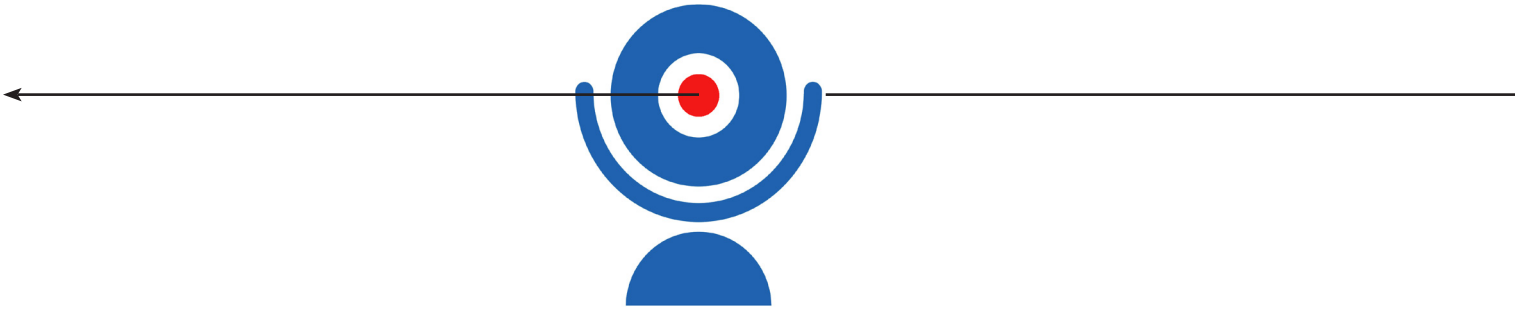
Remote activation software sold to businesses and school districts by private companies has been flagrantly abused. In one prominent case, a school district captured tens of thousands of digital pictures of unsuspecting students.[14] Meanwhile, individual hackers known as "ratters," using software available online for $40 or less, trick unsuspecting victims into installing remote access Trojans (RATs[15]) that can provide full control over the victim's computer, including the ability to activate the webcam.[16] Reflecting the well-documented problem of misogyny on the internet,[17] ratters discuss their conquests on web discussion boards on sites such as hackforums.net, where they dub their victims "slaves" or "slave girls."[18] Sometimes they hold "slave auctions" where they trade access to victims' computers.[19]

Webcams have transformed entertainment, medicine, home security, and many other fields. But they have also been used to spy on people in shocking ways.

The tools of remote access have long been used for legitimate purposes, including by IT departments for remote configuration, monitoring, and maintenance.[20] People regularly use these tools to access software and files on their home computers when they are away from home.[21] Organizations install remote administration software on computers distributed to students or employees to assist in their maintenance or to facilitate recovery in case of theft.[22] Rent-to-own businesses have also used remote administration software to remotely disable rented computers in the event of nonpayment.[23]

Some people unwittingly give ratters access to their webcams by connecting to the internet from their home computer, home security system, or devices such as baby monitors by failing to configure these tools correctly. At a security conference, researchers revealed that they were able to compromise the computers of thousands of users of remote access tools who neglected to set up password protection.[24]

Technology allowing the remote activation of webcams raises important law and policy issues. Remote activation by government entities, private companies, and malicious individuals each raise unique concerns. These concerns include insufficient disclosure and a lack of opportunity for public oversight in the case of government use; incentives for private companies to perform intrusive surveillance in place of the police; and existing laws' failure to adequately protect victims of surreptitious remote activation.



2. WHO'S WATCHING YOU?

Classified documents released to the press revealed that the United States government, along with its "Five Eyes" partners, engages in extensive surveillance of telecommunications networks worldwide.[25] The full scope of such surveillance has never been disclosed. However, the programs that have been revealed are breathtaking in scope. Since May 2006, in its bulk telephony metadata collection program, the U.S. government has collected metadata on "substantially every telephone call in the United States."[26] In another surveillance program, codenamed "Optic Nerve," the U.K.'s Government Communications Headquarters (GCHQ), with the NSA's assistance, captured and stored webcam images from more than 1.8 million Yahoo user accounts worldwide, "including substantial quantities of sexually explicit communications."[27] In addition to intercepting communications, many governments worldwide have the technology to remotely activate webcams.

The scope of government webcam surveillance in the United States is impossible to gauge. In the Foreign Intelligence Surveillance Court, which generally handles requests for electronic surveillance involving foreign intelligence targets (and U.S. citizens who associate with them), proceedings are held in secret and orders are issued in secret.[28] Furthermore, surveillance orders under the Electronic Communication Privacy Act (ECPA) governing domestic electronic surveillance are "kept under wraps in three ways: sealing of court records, delayed notice to the target, and nondisclosure ("gag") orders directed to service providers and their agents."[29] Targets who are not subsequently charged with a crime will often never learn of the surveillance.[30]

Remote webcam activation has also been used by government in the public school setting. Between 2008 and 2010, Information Services (IS) personnel at the Lower

Merion School District (LMSD) outside Philadelphia used remote access software, intended only to be used in cases of theft, to collect a total of 27,428 screenshots and 30,564 webcam photos from student-issued laptops.[31] "This is awesome. It's like a little LMSD soap opera," an IS technician wrote in an email.[32] "I know, I love it!" the district's IS Coordinator responded.[33] The surveillance came to light when Blake Robbins, a 15-year-old student, was confronted by an assistant principal with a webcam photo of him holding what she believed were illegal pills.[34] The student said he was holding Mike and Ike's candy.[35] After Blake and his parents sued the school district, it emerged that school personnel had captured over 400 screenshots and webcam photos via Blake's laptop.[36] Jalil Hasan, another student, found that school personnel had captured over 1,000 images—543 screenshots and 469 webcam photos—gathered over the course of two months via his laptop.[37] The district also collected 3,805 photos and 3,451 screenshots from 12 laptops issued to teachers.[38] The district's gathering of these images continued until the day the Robbins family sued the district.[39] After the story broke, the FBI investigated, but it declined to prosecute any school officials, saying existing laws did not cover this situation.[40]

Blackshades, a RAT, has been used in more than 100 countries to infect more than half a million computers worldwide.

Private businesses also use remote access tools that allow for webcam activation. Such tools are intended to help locate stolen computers or to disable computers if the would-be purchasers fall behind in their payments. PC Rental Agent, a remote access tool providing remote webcam activation capability that was developed for and marketed to the rent-to-own industry, was licensed by more than 1,600 Aaron's, Inc., franchise stores nationwide and installed on over 400,000 computers rented to consumers.[41]

In addition, thousands of individual "ratters" use RATs to gain control over others' computers to allow remote webcam activation.[42] Online discussion boards such as Hack Forums frequently discuss methods of avoiding detection while surreptitiously activating webcams, for instance by targeting computers whose webcams lack an indicator light that could alert the user to the webcam being activated.[43] A single, dedicated ratter can harm a large number of victims, sometimes threatening to leak the surreptitious photos unless the victims send them better nude photos as ransom. Luis Mijangos, a prolific "sextortionist," single-handedly infected 129 computers, netting a total of 230 victims, including 44 juveniles.[44] Jared James Abrahams, who

gained infamy for victimizing Miss Teen USA 2013 Cassidy Wolf by taking photos through her webcam, targeted over 150 victims during his ratting career.[45] According to the FBI, Blackshades, Abrahams' RAT of choice, has been "sold and distributed to thousands of people in more than 100 countries and has been used to infect more than half a million computers worldwide."[46]

3. WHAT TECHNOLOGIES ENABLE DIGITAL PEEPHOLES?

A range of technologies exist to allow governments or individuals to take over a target's webcam. Surveillance software firm Gamma International sells FinFisher, a powerful hacking software suite, to governments worldwide.[47] Marketed as a law-enforcement tool, FinFisher can bypass popular antivirus products, harvest data from the hard drive, capture webcam footage, log keystrokes, and record emails, chats, and Skype calls, all of which it sends to a central command-and-control server.[48] The Milan-based company Hacking Team offers similar software.[49] Gamma and Hacking Team also sell governments devices known as "network injection appliances," which can be installed at an internet service provider (ISP) and used to insert malicious commands into any unencrypted web traffic—a tactic security expert Morgan Marquis-Boire called "hacking on easy mode."[50] Citizen Lab and others have criticized Gamma and Hacking Team for selling these tools commercially, including to repressive regimes such as the government of Bahrain, which has tortured political dissidents.[51] In March 2013, Citizen Lab found FinFisher command-and-control servers in 25 countries, including the United States.[52]

Even without such sophisticated tools, a person's webcam can be accessed remotely. Activating an ordinary computer user's webcam remotely does not require great technical ability. Ratters typically gain unauthorized access to victims' computers by tricking them into opening a seemingly innocuous file that covertly installs a RAT on the victim's computer.[53] The file can be delivered as an email attachment or a popular song or video on a peer-to-peer file sharing network such as BitTorrent.[54] After the RAT is installed, it "phones home" to the ratter's computer and grants the ratter control.[55]

Tricking a computer user into unwittingly installing a RAT is easy to accomplish in practice, even for relatively unskilled users. As journalist Nate Anderson noted, "Calling most of these guys 'hackers' does a real disservice to hackers everywhere; only minimal technical skill is now required to deploy a RAT and acquire slaves."[56] Sometimes, activating a webcam remotely requires no "hacking" at all: using only standard instant messaging software, which he configured to automatically accept incoming video calls, and aiming his webcam before leaving the room, Rutgers student Dharun Ravi was able to activate his own webcam remotely and spy on Tyler Clementi during Clementi's romantic encounter with a same-sex partner.[57]

Sometimes, activating a webcam remotely requires no "hacking" at all.

While many webcams come with a connected light that turns on when the webcam is active, not all do, and reports have shown that it is technically possible to activate many webcams without triggering the indicator light.[58] Online ratter discussion forums contain threads discussing laptop models with no indicator light, and possible methods of activating a webcam without triggering the light, in order to avoid alerting the victim to suspicious activity.[59] According to a former FBI official, "the FBI has been able to covertly activate a computer's camera—without triggering the light that lets users know it is recording—for several years."[60] Johns Hopkins University researchers demonstrated that it was possible to reprogram a MacBook microcontroller to allow the webcam and indicator light to operate independently of one another, even though it was designed specifically to prevent this.[61]

HOW DO OUTSIDERS TURN YOUR WEBCAM AGAINST YOU?

Ratters, people who use remote access Trojans (RATs) to take control of individual computers and webcams from afar,[1] have a lively marketplace and advice headquarters at message boards like hackforums.net. There, ratters—stereotypically and likely not inaccurately young men—buy and sell "slaves," people whose computers and webcams have been commandeered for the men's vicarious enjoyment. Ratters also trade tips about "slaves" and the best ways to spread RAT software.

While virtually all computers are vulnerable in some way or other to top attackers, ratters, many of whom are novices, often rely on one of a few tricks to convince users to infect themselves. There are some common ways, and luckily, they are often easily avoidable.

FAKE MEDIA

Torrents are a staple of the internet, particularly for those seeking to download media, research, and software. Torrents are small files that help users locate and download content from many users at once using BitTorrent, a protocol designed to enable peer-to-peer sharing and downloading. A report by analytics company Musicmetric, for example, found that in the first six months of 2012 there were 405 million music releases downloaded around the world with the help of torrent files and BitTorrent.[2] Ratters take advantage of the proliferation of torrent search engines by disguising RATs as popular songs and uploading them to the internet for torrent sites.

Ratters search the charts of popular torrented music and upload their RATs named after these songs to torrent sites. Ratters pay attention to ways of gaming the system, including evading torrent sites' internal controls by not uploading too many files soon after registering, using multiple accounts to provide fake positive feedback for a potential download (that is actually infected with software to allow the ratter to turn on your camera), or uploading legitimate files first to boost reputation. Ratters may upload a legitimate version of a song along with a RAT with a name like "PASSWORD TO UNLOCK" or "ESSENTIAL: READ ME FIRST." A user who clicks the disguised RAT .exe may end up with access to the original file but also can be infected at the same time. It's devious, but luckily it's easy to spot. A rule of thumb—if a torrent download requires you to click a link or run a separate file in order to access whatever you were after, it's better to steer clear.

"OMG I CAN'T BELIEVE THAT PIC OF U!!!"

Facebook, Twitter, Chatroom, and Ad Spamming

If you're active on any social networks or chatrooms, chances are you've come across a message and link reading something like, "OMG I can't believe this picture of u!" These spam messages, which, sites like Twitter have fought by limiting the types of links that can be sent via the service's Direct Message function, are one way that ratters recommend spreading their wares. Sometimes, the spam messages will come from people you actually know whose computers have been infected and turned into zombie transmission devices. Alternately, websites and ads designed to look like legitimate products such as the Firefox browser or anti-spyware software may also carry RATs. As librarian and privacy advocate Alison Macrina Tweeted, a Google or Bing search for Firefox actually returned multiple fake Firefox downloads ahead of the actual Firefox website.[3] (No such result appeared in the privacy-friendly DuckDuckGo search engine).

Some lessons are to inspect URLs to make sure they link to the legitimate version of software. You can submit files or links to malware analyzer Anubis[4] or do a web search for the names of unfamiliar programs to check for reports that they are infected. And finally, never click (at least not without responding to the sender for more information) an out of the blue message from a friend on a social network promising a link to a "Crazy Pic" or something like it.

SPEAR PHISHING

While uploading popular songs with associated malware to torrent sites is a common technique to obtain "slaves," there are also tutorials for infecting a specific person, perhaps someone a ratter knows in real life. Without the randomness of posting a torrent and RAT to a website, the creepier process of targeted infection using information from someone's life—"spear phishing"—is more elaborate but also in many ways more dangerous. In both these cases, however, a ratter needs to trick someone in to clicking a link to install the RAT server on their computer.

One example discussed on hackforums.net outlines a hypothetical attack on a college student. In this attack, which the poster's notes can be modified to suit different factual situations, a ratter will reach out to a new student pretending to be a student organization offering free textbooks. The email seems legitimate enough, there may be a flimsy website set up for the fake student group, and the files that eventually get sent are actual textbooks, pirated by the ratter for the purposes of the attack. When there is enough trust between the parties, the fake student organization sends the textbooks along with Readme.txt that tells the student to run a fake "PASSWORD GENERATOR" .exe file, included along with the password protected textbooks. When the victim runs the password generator, they are actually running the RAT, but to prevent any concern, the password generator also provides a legitimate password for the textbook pdfs.

This trade is a bad one for the victim, as their computer and privacy are compromised. Use common sense—it's pretty unlikely that a student organization would randomly email new students and offer free versions of copyright-protected textbooks, no matter how convincing the backstory.

THE MOST DANGEROUS GAME

While each of these methods develops in its own way, a shared aspect is that they rely on tricking someone into clicking a link to run a file that installs and sets up the RAT. Other methods work the same way, with added layers of nuance or difference. One way involves hosting a website featuring a fake video game, where clicking a button in the game will load a fake "error" screen and eventually lead to a download screen for a software update to "fix" the problem. The same website might contain a link to a fake YouTube video advertising the game, where pressing "play" triggers an error designed to trick the user into thinking he or she has to download some update in order to access (actually the RAT). As a rule, reputable websites tend to clearly advertise and contextualize when they are going to offer a download link, so a random download accompanying a click on a video or game should be distrusted.

NOTES

1 Nate Anderson, "Meet the Men Who Spy On Women Through Their Webcams," *Ars Technica*, March 10, 2013, http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/.

2 Enigmax, "Top Bittorrent Countries in the World, Top Torrent Towns in the UK," *Torrent Freak*, September 17, 2012, https://torrentfreak.com/top-bittorrent-countries-in-the-world-top-torrent-towns-in-the-uk-120917/.

3 Alison Macrina, Twitter (Aug. 22, 2014, 11:48 AM), https://twitter.com/flexlibris/status/502890161840328705.

4 Anubis, https://anubis.iseclab.org/ (last modified September 4, 2014).

4. ASSESSING WEBCAM ACTIVATION IN A BROADER LEGAL CONTEXT

The proliferation of webcams raises serious privacy concerns. The Fourth Amendment of the U.S. Constitution bars unreasonable searches and seizures, providing restrictions on the remote activation of webcams by government actors. The constitutional right to privacy provides additional protection. Private actors, while generally not bound by constitutional limits, are subject to a variety of criminal and civil laws that could potentially be used to restrain their use of remote webcam activation technology.

The Fourth Amendment to the U.S. Constitution generally requires law enforcement officers to obtain a warrant to perform a search or seizure, and in obtaining the warrant, to state with particularity the place to be searched, and the persons or things to be seized.[62] The U.S. Supreme Court has held that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[63] Furthermore, courts have recognized that "video surveillance can result in extraordinarily serious intrusions into personal privacy," prompting heightened scrutiny.[64] Webcams are often positioned where they can reveal intimate details in the home, where "Fourth Amendment interests are at their strongest."[65] And because many computers are shared, the remote activation of a webcam by law enforcement poses a substantial risk of invading the privacy of unintended third parties of no interest to any investigation. The Fourth Amendment applies only to the government and not to private businesses or individuals, unless the business or individual is acting as an agent of the government; if a company independently remotely activates a webcam and gives the photos to the police, the person photographed has no constitutional protection.

The federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, makes it a

federal crime to intentionally access a computer without authorization.[66] The statute is broad in scope and has been used to prosecute people for acts ranging from accessing workplace computers in violation of corporate policy to collecting and disseminating subscriber information made available by AT&T on its public web server.[67] However, the statute offers little relief to victims of remote webcam activation because it requires showing a minimum $5,000 in monetary damages in order to bring a civil claim.[68]

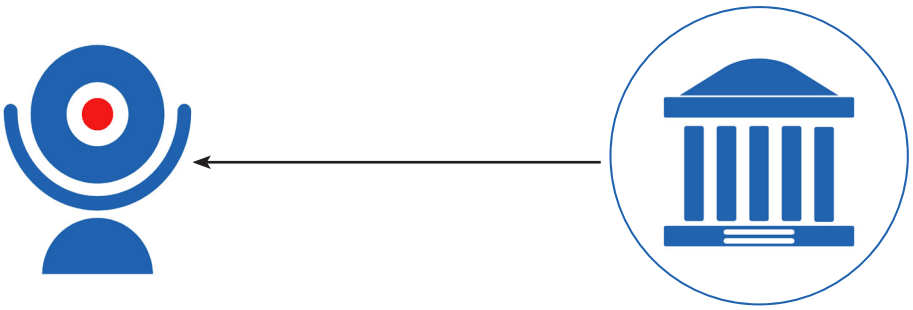
The Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2511 *et seq.*, an amendment to the Wiretap Act, prohibits the interception, use, or disclosure of electronic communications without the consent of at least one party. The Act does not require the permission of the person being photographed, if the other party authorizes the snooping. And even in situations where the ECPA could potentially have been applied to remote webcam activation, courts have been reluctant to find remotely capturing screenshots or activating a webcam to be a violation.[69] The ECPA is meant to cover surreptitious eavesdropping on electronic communications as they occur. Courts have held that interception of an electronic communication must occur while the communication is "in flight" in order to be covered.[70] Applying this metaphor, courts have held that webcam photos taken through the use of remote access software cannot be "interceptions" because they are the creations of the person activating the webcam, not intercepted communications of the person photographed.[71]

The FTC has held that remote webcam activation, without notice to consumers, is an unfair business practice.

The Federal Trade Commission (FTC) has a broad mandate to prevent unfair business practices. Section 5 of the FTC Act, 15 U.S.C. § 45, directs the Commission to prevent "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." In keeping with this directive, the FTC has taken enforcement actions against companies for spying on their customers and failing to provide notice of possible webcam surveillance.[72] The FTC has indicated that remote webcam activation, without notice to consumers, is an unfair business practice because the disclosure of intimate details of private and family life can put consumers at risk of physical harm, the collection of bank account and other sensitive information can cause financial harm, and both of these can impair consumers' peaceful enjoyment of their homes.[73]

Finally, remote webcam activation raises state criminal and civil issues, particu-

larly invasion of privacy—a claim raised in almost all state-level criminal and civil actions involving remote webcam activation.[74] Invasion of privacy goes to the core of what is troubling about remote webcam activation, and a claim based on invasion of privacy will often succeed where, for technical reasons, others fail. In some states, such as California, the right to privacy is part of the state Constitution, providing the basis for the State Attorney General to prosecute individuals and companies that use remote access technologies to turn on webcams without consent.[75] In addition, all fifty states also have criminal laws prohibiting unauthorized computer access; some of those laws do not impose a money damages requirement in order to bring a civil suit[76] and thus may help victims of webcam snooping.



5. LEGAL CONCERNS IN THE REMOTE ACTIVATION OF WEBCAMS BY THE GOVERNMENT

The government's use of remote webcam activation and other forms of electronic surveillance is restricted by the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable searches and seizures. The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[77]

This Amendment entails a "particularity requirement," meaning that the police can only search a specific place for a specific item or items of contraband, and may not simply perform broad, general searches to see what turns up, and a "minimization requirement," meaning that the government must take all possible steps to avoid searching unrelated third parties. In addition, relevant to the specific issue of remote webcam activation, courts have held that video surveillance, in contrast to other forms of surveillance, is so uniquely intrusive that it requires particularly searching judicial scrutiny.[78]

The ECPA sets forth the specific requirements for the government to obtain a warrant for electronic surveillance.[79] In 2006, Congress expanded the electronic surveillance resources at the disposal of the police by passing the Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001-10, which requires communications providers to cooperate with law enforcement surveillance efforts and to provide officers with access to their systems and facilities in certain circum-

stances. Similarly, the CFAA, which broadly outlaws unauthorized computer access, contains the exception that it "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States." These statutes reflect Congress' judgment that electronic surveillance, under court supervision, can be an important investigative tool.

However, remote webcam activation, as a uniquely intrusive method even among techniques of electronic surveillance, raises serious constitutional questions. The webcam can capture the image of anyone using the computer, not only the person of interest in the investigation, and thus poses serious risks for infringing on the rights of innocent third parties. Moreover, in a situation where the location of the computer itself is unknown, surveillance might ensnare the wrong computer entirely.

In April 2013, U.S. Magistrate Judge Stephen W. Smith[80] denied an application by the FBI to install remote access software on an unspecified computer in an unknown location, and to perform remote electronic surveillance, including by activating its webcam.[81] Judge Smith held that he was not authorized to issue such a warrant under the territorial limits imposed by Rule 41(b) of the Federal Rules of Criminal Procedure,[82] that the request risked affecting too many unrelated third parties to meet the Fourth Amendment's specificity requirement,[83] and that the request failed to meet the heightened constitutional requirements imposed on video surveillance because of its unique intrusiveness.[84]

Remote webcam surveillance poses serious risks for infringing upon the privacy rights of innocent third parties.

In the case presented to Judge Smith, unidentified individuals gained unauthorized access to a victim's email account, and used information gathered to access his bank account.[85] The Internet Protocol (IP) address of the computer accessing the victim's account appeared to indicate that the computer was in a foreign country. The victim discovered the breach and took steps to secure his email account. Following this, an email account with an address nearly identical to the victim's was used to attempt a sizable transfer of funds from his account to a foreign bank account. The FBI began an investigation.

The FBI then sought a warrant allowing it to target an unknown computer with remote access software by sending it to the email address used by the identity thieves.[86] The software would allow the government to search and extract various

data from the thieves' computer's hard drive, random access memory (RAM), and other storage media, to obtain latitude and longitude coordinates for the computer's location, to take screenshots, and to activate its webcam in attempt to identify the computer's location and users.[87]

Judge Smith held that he lacked jurisdiction even to issue such a warrant.[88] Under Federal Rule of Criminal Procedure 41(b):

> At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district[.]

The government argued that Rule 41(b)(1) gave Judge Smith authority to issue the warrant because the data gathered remotely would be examined in the territory over which he had authority—the Southern District of Texas.[89] Because its agents would not need to leave the district in order to obtain and view the data gathered, the government argued, the data would effectively become "property located within the district" under Rule 41(b)(1).[90]

Judge Smith rejected this argument, holding that he was precluded from issuing a warrant to perform a search in an unknown territory. According to Judge Smith, the government's logic "would permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district."[91] Judge Smith noted that the request was actually two-fold, consisting first of a search for the target computer itself, and then a search within the target computer for digital information stored on, or generated by, the target computer.[92] Judge Smith explained that the proposed search for information on the target computer "takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name."[93] Hence, allowing these searches to occur anywhere so long as the data and images gathered were examined in the issuing district would nullify the limits set by Rule 41(b)(1).[94]

Additionally, Judge Smith found that even if he had authority to issue the warrant, it would fail under the Fourth Amendment's requirements of particularity and minimization. The Fourth Amendment requires that a search warrant "particularly [describe] the place to be searched, and the persons or things to be seized."[95] As-

suming that the computer would be targeted with spyware sent via the counterfeit email address—since the warrant application did not disclose the targeting method—Judge Smith reasoned that the malware could infect the computers of other individuals who happened to share the target email address.[96] The malware could also infect uninvolved computers, such as a public computer at which the intended target happened to check his or her email. Furthermore, the search could be routed through one or more unrelated computers if the target computer's IP address were "spoofed." As the court explained:

Even if the Government could meet the minimization and particularity requirements of the Fourth Amendment, webcam surveillance would likely not pass constitutional muster.

> What if the Target Computer is located in a public library, an internet café, or a workplace accessible to others? What if the computer is used by family or friends uninvolved in the illegal scheme? What if the [target] email address is used for legitimate reasons by others unconnected to the criminal conspiracy? What if the email address is accessed by more than one computer, or by a cell phone and other digital devices?[97]

The government's application offered only the conclusory statement that "the method in which the software is added to the target computer is designed to ensure that the [persons] committing the illegal activity will be the only individuals subject to said technology."[98] The court found this assurance insufficient to satisfy the particularity requirement.[99]

Furthermore, according to Judge Smith, even if the government had met the minimization and particularity requirements, its request for webcam surveillance would still likely fail to pass constitutional muster. Courts have held that the Fourth Amendment imposes a special, heightened standard of scrutiny on requests to perform video surveillance. In *United States v. Cuevas-Sanchez*,[100] the U.S. Court of Appeals for the Fifth Circuit described video surveillance as "a potentially indiscriminate and most intrusive method of surveillance," and set forth heightened standards for a warrant authorizing video surveillance:[101]

> [A] search warrant authorizing video surveillance must demonstrate not only probable cause to believe that evidence of a crime will be captured, but also should include: (1) a factual statement that alternative investigative methods have been tried and failed or reasonably ap-

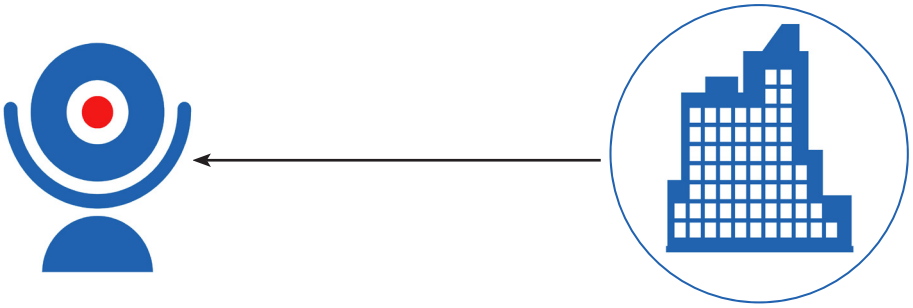
> pear to be unlikely to succeed if tried or would be too dangerous; (2) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (3) a statement of the duration of the order, which shall not be longer than is necessary to achieve the objective of the authorization nor, in any event, longer than 30 days, (though extensions are possible); and (4) a statement of the steps to be taken to assure that the surveillance will be minimized to effectuate only the purposes for which the order is issued.[102]

Judge Smith held that the government's request to perform webcam surveillance failed to meet these heightened standards because it failed to adequately consider less invasive alternatives or minimize its scope.[103] Instead, the application stated, in language reciting the legal standard, that alternative methods "reasonably appear to be unlikely to succeed if tried or would be too dangerous."[104] However, in a separate warrant application the government had sworn that internet service provider (ISP) records would likely reveal the suspects' identities and locations.[105] In light of this, Judge Smith rejected the government's assertion that alternative methods to webcam surveillance would likely be unsuccessful if tried or too dangerous.[106] Further, the government asserted in its application that the software was designed to capture only "the minimal necessary information needed to identify the location of the Target Computer and the user," but the warrant application described a wide variety of data to be extracted, including "Internet browser history, search terms, e-mail contents and contacts, 'chat', instant messaging logs, photographs, correspondence, and records of applications run."[107] Judge Smith found that the volume of information the government intended to collect undermined its assertion that the intended surveillance would be minimized.[108]

In response to Judge Smith's adverse ruling, in September 2013 the U.S. Department of Justice (DOJ) wrote to U.S. Circuit Judge Reena Raggi, Chair of the Advisory Committee on the Rules of Criminal Procedure, to propose an amendment to Rule 41(b) to loosen the territorial requirements for warrants in searches for electronic storage media.[109] The DOJ proposed adding a sixth subsection to Rule 41(b): "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant, to be executed via remote access, for electronic storage media or electronically stored information located within or outside that district."[110] In May 2014, the Advisory Committee recommended that this proposed amendment be submitted for public comment.[111] As of yet, the rule has not

been amended.

Even in the event of such a rule change, however, any request by law enforcement to remotely activate a webcam would suffer from the same constitutional deficiencies as the warrant application in the Texas case. The particularity problems noted by Judge Smith—i.e. , the high likelihood of a remote search ensnaring unrelated computers and files and uninvolved individuals—appear inherent in any government remote activation operation. As the ACLU has noted, "the particularity problems likely to be raised by remote access search warrants are entirely predictable."[112] Likewise, there appear to be few situations, if any, in which a request to install software for remote webcam surveillance could meaningfully be "minimized to effectuate only the purposes for which the order is issued."[113] Furthermore, the proposed rule change does not address the enhanced constitutional requirements for video surveillance, which Judge Smith held precluded remote webcam activation. Remote activation of webcams by government runs afoul of the principles of the Fourth Amendment. Even though Judge Smith denied a warrant to the FBI to remotely activate a webcam, it is impossible to learn whether other judges in secret hearings are authorizing such warrants. Consequently, to ensure that the Fourth Amendment principle is followed, it may be necessary to adopt a statue to specifically forbid webcam activation by government entities.



6. LEGAL CONCERNS IN THE REMOTE ACTIVATION OF WEBCAMS BY PRIVATE COMPANIES

Private companies have also used tools allowing remote webcam activation, in particular for anti-theft purposes. Absolute Software reports that it successfully recovers three out of four laptops reported stolen by purchasers of its LoJack remote access tool.[114] PC Rental Agent, another such tool, was developed in part as a theft recovery tool by a computer programmer and owner of several rent-to-own stores. Proponents of the tools claim that they are useful in recovering stolen computers by providing the ability to determine who is using the computer believed or reported to be stolen.[115] But companies have abused these tools once installed, resulting in litigation and FTC enforcement actions.

Private companies face no constitutional obstacles to remotely activating webcams, since the Constitution applies only to the government. The Computer Fraud and Abuse Act (CFAA) is also of little use to most victims of private webcam surveillance. Under the CFAA, a private plaintiff must be able to show loss during a one-year period of at least $5,000 in order to bring a civil suit under the statute,[116] and the harms of webcam spying are largely dignitary, emotional, and psychological rather than monetary. Potentially more helpful to plaintiffs, the ECPA imposes safeguards against electronic surveillance and provides a private right of action for actual or statutory damages.[117] However, at least one judge who considered the question has doubted that remotely taking screenshots or activating a webcam could constitute a forbidden "interception" under the ECPA.[118]

State law can provide potential recourse in some instances. Almost all U.S. states recognize an actionable right to privacy, either by statute or common law.[119] Among common law privacy claims, the common law tort of intrusion into seclusion is particularly pertinent to the issue of webcam spying, in some cases along with public

disclosure of private facts. Additionally, California's constitution expressly provides a right to privacy under which Californians may bring a civil action.[120] Hence, in most U.S. states, people who are spied on by private parties through their webcams could potentially have legal recourse under the state privacy laws.[121] But people may not realize they have these rights and judges may not be willing to enforce them in situations involving an investigation into a purported theft.

The Application of Federal Wiretap Statutes to Corporations

The rent-to-own industry was an early adopter of remote access tools, including webcam activation capabilities. Typically situated in poor, largely-minority neighborhoods, rent-to-own stores sell goods on installment at total prices often dramatically larger than those at traditional stores.[122] Consumer advocates have long condemned rent-to-own stores for charging higher costs for the same goods than more affluent consumers pay at traditional stores, depriving their customers of key consumer protections, and taking advantage of people less able to evaluate transactions for fairness.[123] Furthermore, scholars have documented how new surveillance technologies have disproportionately targeted people of color and the poor (sometimes with these groups used as testing grounds for surveillance tools later introduced into the broader population).[124] In keeping with this trend, rent-to-own stores were at the center of one of the first national scandals involving remote webcam activation.

The rent-to-own industry was an early adopter of remote access tools including webcam activation capabilities.

In December 2010, Christopher Mendoza, a manager at a franchise of Aaron's, a rent-to-own chain, visited the home of Brian and Crystal Byrd to confront them about being behind on payments for their laptop.[125] Mendoza confronted Brian Byrd with a screenshot and webcam photograph of him taken an hour earlier via the computer Byrd was using to play online poker.[126] Brian asked how Mendoza had obtained the images, and Mendoza told him about PC Rental Agent, a remote access tool installed on the computer.[127] Byrd produced a receipt stating that the computer was paid in full, and Mendoza left.[128] Later, Crystal Byrd recalled that the computer's webcam light had come on intermittently in the preceding weeks, including on one instance in which she was using the computer wearing only her underwear.[129] Later, the Byrds learned that their computer was accessed using PC Rental Agent approxi-

mately 347 times over a one-month period in November and December 2010.[130]

Years earlier, beginning in 2007, Aaron's franchisees began installing PC Rental Agent on computers prior to rental, without informing customers.[131] PC Rental Agent included a "kill switch" that would disable the computer in cases of nonpayment.[132] It also included "Detective Mode," which displayed a fake registration screen to solicit personal information from the computer user, and allowed stores to surreptitiously collect keystroke logs, screenshots, and webcam photos.[133] While designed to provide stores with "gotcha" evidence against customers who reported computers stolen but continued to use them, a former manager at an Aaron's franchise testified that more often than not, the individuals against whom PC Rental Agent was used were not in default.[134] PC Rental Agent captured sensitive information from these customers, including names, addresses, phone numbers, Social Security numbers, and financial information.[135] The former manager testified that she also saw hundreds of webcam photos of individuals and that managers would "basically sit back there and joke about it."[136]

The Byrds filed a class action lawsuit against Aaron's, Inc. , Aspen Way Enterprises (the Aaron's franchise from which the Byrds had purchased the computer), other franchisees using PC Rental Agent, and DesignerWare LLC (the company that had created PC Rental Agent and licensed it to Aspen Way and other franchisees). The Byrds asserted claims under the ECPA, Section 2511, which prohibits the interception, disclosure, and use of electronic communications, and Section 2512, which prohibits the use of devices having the primary purpose of intercepting electronic communications. The Byrds alleged that the defendants had unlawfully intercepted screenshots, key logs, and webcam photos under Section 2511, and that PC Rental Agent was unlawful under Section 2512 as a device for intercepting electronic communications.[137] They also asserted that the defendants accessed their computer without authorization in violation of the CFAA.[138]

A rent-to-own store covertly accessed a customer's computer approximately 347 times over the course of 30 days.

DesignerWare and Aaron's filed motions to dismiss, arguing that the Byrds lacked standing and that they had failed to state a claim on the merits.[139] Specifically, they argued that the Byrds had failed to plead facts showing the contemporaneous transmission of an electronic transmission under ECPA Section 2511, that there was no private right of action under ECPA Section 2512, and that they had failed

to plead facts showing the minimum of $5,000 in "damage" or "loss" to support a claim under the CFAA.[140] Aaron's further argued that the Byrds' pleadings contained allegations against only the franchisee defendants, and that there was no secondary liability under the statutes that could implicate Aaron's.[141]

Section 2511 of the ECPA criminalizes, with certain exceptions, the actions of anyone who:

> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; . . .
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection. . . .

An "electronic communication" is defined generally in 18 U.S.C. § 2510(12) as:

> 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. . . .

"Intercept," under 18 U.S.C. § 2510(4), means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Section 2520 provides a private right of action to anyone whose electronic communications are intercepted in violation of Section 2511.

A key disagreement between the parties concerned whether PC Rental Agent "intercepted" electronic communications within the meaning of Section 2511. Aaron's argued that various U.S. Circuits, including the Third Circuit, have held that an electronic communication must be intercepted contemporaneously with its transmission in order to give rise to liability under Section 2511.[142] Screenshots and keystrokes, Aaron's argued, are not captured during transmission because they capture

a static image on the Byrds' computer screen and a set of letters previously typed. Similarly, Aaron's argued that the webcam photo of Brian Byrd was created by Detective Mode itself and therefore not a communication of Brian Byrd's that was captured during transmission.[143] In response to these arguments, the Byrds argued that Brian Byrd was transmitting data back and forth with a poker website, as reflected on the computer screen, at the time the screenshot and webcam photo were taken.[144] The Byrds' response brief offered screenshots captured by PC Rental Agent, along with timestamped emails reflecting the receipt of emails by Aspen Way (the Aaron's franchise) reporting the keystrokes shown as evidence of contemporaneous interception.[145]

Early in the proceedings, the presiding magistrate judge found that the capture and transmission by PC Rental Agent of a screenshot and keystrokes entered by Brian Byrd constituted "interceptions" under Section 2511 because they occurred contemporaneously with their transmission over the internet.[146] The magistrate judge further found that the screenshot and keystrokes constituted "electronic communications" under 18 U.S.C. § 2510(12). However, the magistrate judge found that the webcam photo did not constitute an "interception" within the meaning of Section 2511 because Brian Byrd, despite being pictured, did not take or transmit the photo.[147]

Later, reviewing the magistrate's report, the district judge adopted the finding that the webcam photo was not an "interception" under Section 2511; he also expressed skepticism as to whether the captured keystrokes and screenshots constituted "interceptions," but allowed those issues to proceed to discovery for factual development.[148] In March 2014, the court dismissed all franchisee defendants except Aspen Way on standing grounds, and denied the Byrds' motion for class certification.[149] The parties remaining in the case continue to dispute the issue of what constitutes "interception" under the ECPA, and the denial of class certification is currently on appeal.[150] Separately, in June 2014, two lawyers who were rental computer customers of Aaron's filed a new lawsuit against Aaron's over PC Rental Agent, asserting Georgia law invasion of privacy and computer trespass claims.[151]

The *Byrd* case highlights a significant shortcoming in the law: in the court's view, the ECPA prevented Aspen Way from intercepting the Byrds' electronic communications, but not from taking over their computer itself and invading their privacy in their home. Aspen Way would have faced ECPA liability for intercepting a photo of Crystal Byrd in her underwear, but would not face liability under the statute for

hijacking her computer and taking one with her webcam. In part, this is because of the weakness of the "flight" metaphor: what does it mean for an electronic communication to be "in flight?" Does the computer's relaying data from the internet to the laptop screen count? What about keystrokes that, when entered, are immediately recorded and sent to a third party server by a program on the computer? The "flight" metaphor in the ECPA context is a red herring that leads to absurd results; courts should take a step back and consider the bigger picture, rather than getting hung up on flawed metaphors for "interception" when considering ECPA claims.

The Application of Federal Trade Commission Actions to Corporations

Private companies seeking to perform webcam surveillance are also subject to the FTC's authority to enforce the federal prohibition on unfair and deceptive business acts and practices. The FTC Act, 15 U.S.C. § 45(a)(1) prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce," and gives the FTC the authority to investigate infractions and commence enforcement actions against companies who engage in unfair or deceptive business practices.[152] These include acts or practices which are "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[153] In the software context, this includes cases in which a product fails to work as advertised or to follow its own privacy policy. It can also encompass situations in which there is no misrepresentation to consumers by the developer, but where the software acts in ways so negligent or contrary to consumer interests as to be inherently unfair, such as by failing to encrypt a customer's financial or medical information while transmitting it over the internet.[154]

After the PC Rental Agent scandal came to light, the FTC launched investigations of Aaron's, various Aaron's franchisees (including Aspen Way Enterprises, where Brian and Crystal Byrd purchased their laptop), and DesignerWare and its principals, all resulting in formal complaints.[155] The complaints charged that the use of PC Rental Agent's information-gathering, monitoring, and surveillance capabilities without prior disclosure to customers constituted unfair business practices.[156]

The FTC complaints centered on the charge that it was an unfair and deceptive business practice to use PC Rental Agent to gather information from customers without their knowledge.[157] Specifically, in its complaint against Aspen Way, the

FTC alleged:

> Aspen Way has obtained data via Detective Mode that has revealed private, confidential, and personal details about the computer user. Keystroke logs have displayed usernames and passwords for access to email accounts, social media websites, and financial institutions. Screenshots have captured additional confidential details including medical records, private emails to doctors, employment applications containing Social Security numbers, bank and credit card statements, and discussions of defense strategies in a pending lawsuit. Webcam pictures have photographed not only the computer's user, but also anyone else within view of the camera. In numerous instances, Aspen Way has obtained pictures taken secretly inside the computer user's home. These have included images of minor children and individuals not fully clothed. . . .
>
> Aspen Way's gathering of private and confidential information about individuals causes or is likely to cause substantial harm to customers. Because of Aspen Way's intrusion, customers are at risk of harm from exposure of their personal, financial account access, and medical information. Consumers are actually harmed by Aspen Way's unwarranted invasion into their homes and lives, and its capture of the private details of individual and family life, including, for example, images of visitors, minor children, family interactions, and partially undressed individuals. Secretly collecting such data can cause consumers financial and physical injury and impair their peaceful enjoyment of their homes. Consumers cannot reasonably avoid these injuries because Detective Mode is invisible to them. The harm caused by Aspen Way's unauthorized gathering of confidential consumer information is not outweighed by countervailing benefits to consumers or to competition; indeed, in this context, where rent-to-own stores have alternative effective methods of collection, e.g. , using PC Rental Agent to remotely disable the computer, there are no legitimate benefits to respondent or to the public.[158]

The complaints against DesignerWare and Aaron's contained nearly identical language.[159] The FTC further alleged that it was unfair and deceptive to use PC Rental Agent to display a fake registration window to collect the user's name, address, email address, and phone number, in order to find, require payment for, or repossess a computer.[160] The FTC alleged that this was deceptive because consumers' information was collected under false pretenses, and unfair because consumers were "deprived of the ability to control who has access to their contact information and how they are contacted."[161]

While company-owned Aaron's stores did not use PC Rental Agent, the FTC al-

leged that Aaron's had nonetheless engaged in unfair and deceptive business practices because it knew that franchisees had licensed PC Rental Agent and installed it on computers rented to consumers.[162] Aaron's knew this, it alleged, because senior executives had given franchisees permission to access the DesignerWare website for purposes of implementing PC Rental Agent, despite an Aaron's IT employee's assessment of the software as "very intrusive."[163] Aaron's provided franchisees with troubleshooting advice for installing PC Rental Agent, and provided step-by-step installation instructions in a company newsletter and on its website.[164] Aaron's could have prevented its franchisees from using PC Rental Agent because its franchise agreement allowed it to "terminate a franchisee that breaches any Aaron's policy or practice or that violates federal, state, or local laws, regulations, or ordinances."[165] Indeed, Aaron's policy prohibited unlawful computer use and mandated fair collection practices.[166]

The FTC enforcement actions resulted in settlement orders with each company.[167] The settlement orders prohibit the companies from using any "monitoring technology"[168] to gather information or data from any computer rented to a consumer, and prohibit DesignerWare from "licensing, selling, or otherwise providing third parties with monitoring technology for installation or activation on computers rented to customers."[169] The prohibited "monitoring technologies" include remote activation of the webcam.[170] The orders further prohibit the gathering of information from consumers using any "geophysical location tracking technology"[171] unless "the computer user is provided clear and prominent notice at the time the computer is rented and immediately prior to each use of the geophysical location tracking technology."[172] However, the orders allow monitoring and geophysical location tracking technologies to be used when a computer is reported stolen and a police report has been filed stating that the computer was stolen.[173]

The orders also prohibit the companies from using a fake software registration window to gather consumer information.[174] Specifically, the orders prohibit "making, or assisting others to make, any false representation or depiction in any notice, prompt screen, or other software application appearing on the screen of any computer that results in gathering information from or about a consumer, including without limitation location information."[175] The order against Aaron's further requires the company to engage in oversight and monitoring of its franchisees to prevent their engaging in prohibited practices.[176]

In sum, the FTC found PC Rental Agent to be unfair and deceptive to consum-

ers because it gathered their personal information under false pretenses, surveilled them without notice, and sent their data insecurely to Aaron's servers. PC Rental Agent's webcam activation tool was designed as a "gotcha" tactic to catch thieves in the act without tipping them off; as its creator testified, it depended on the customer not having knowledge of its existence. The use of remote webcam activation tools by businesses will likely often involve unfair and deceptive acts and practices prohibited by the FTC Act.

Police Work by Private Companies

Investigative collaborations between private companies and law enforcement can blur the line between state and private action, with important legal implications. Because private companies are not bound by the constitutional rights of individuals that limit what the police can do, companies can currently take investigations into their own hands and simply hand the evidence over to law enforcement. There is no Fourth Amendment protection from a search or seizure performed by a private individual even if that search or seizure is unreasonable provided that the private citizen is not acting as an agent of the state.[177] This arrangement holds clear appeal for both the company and law enforcement. Private companies can take investigative actions that police are either forbidden entirely from undertaking or cannot undertake without time-consuming paperwork and judicial scrutiny. And law enforcement officers have long enjoyed the judicial rule that they are not required to "avert their eyes" from evidence third parties present to them so long as there is not a preexisting agency relationship.[178] Thus, surveillance by a private company gathering evidence for police can substantially expedite an investigation. But in the case of potentially invasive techniques such as remote access software, it is questionable whether a private company should be able to do what amounts to police work, without the constitutional constraints that apply to the police.

When highly invasive tactics like remote webcam spying are used, a private company may improperly be performing what amounts to police work.

Susan Clements-Jeffrey, a substitute teacher at an alternative school in Springfield, Ohio, purchased a laptop from a ninth-grade student who told her that he had been given a new one and no longer needed it.[179] In fact, it was a stolen laptop that belonged to the school district where she worked and he was a student.[180] The dis-

trict had installed LoJack for Laptops, a remote access software developed by Absolute Software, Inc. , that gave Absolute investigators the ability to remotely access the computer, capture keystrokes, and take screenshots.[181] The district reported to Absolute that the laptop was stolen, and Kyle Magnus, a "theft recovery officer" for Absolute, used Absolute's remote access tool to gather information from the laptop including keystrokes and screenshots.[182] Some of the screenshots, taken while Clements-Jeffrey was using her webcam, displayed her partially undressed and in intimate positions while chatting with her boyfriend, Carlton Smith.[183] Magnus passed the information along to local police, who in turn used the explicit screenshots to berate and humiliate Clements-Jeffrey while arresting her for possessing the stolen laptop.[184] One of the policemen told Clements-Jeffrey that the pictures were "disgusting" and that she was stupid for sending sexually explicit video by webcam, and explained how LoJack had allowed them to track the computer and monitor her communications.[185]

Clements-Jeffrey and Smith sued the City of Springfield, the police officers, Absolute Software, and Magnus.[186] Clements-Jeffrey and Smith sought relief against the police officers under 42 U.S.C. § 1983, which provides a private cause of action for constitutional violations, claiming that the search of her apartment had violated her rights under the Fourth and Fourteenth Amendments.[187] Clements-Jeffrey and Smith also alleged that the police, the City, and Absolute had violated the ECPA and the Stored Communications Act (SCA), and that the police and Absolute had intentionally invaded her privacy under the common law by obtaining the images from her computer.[188] The defendants moved for summary judgment on all claims except the § 1983 claim relating to the search of Clements-Jeffrey's apartment.[189]

Absolute argued that each of the plaintiffs' claims failed as a matter of law because Clements-Jeffrey should have known the laptop was stolen, and Clements-Jeffrey and Smith could not reasonably expect their conversations on a stolen laptop to remain private.[190] The court applied a two-factor test to determine whether Clements-Jeffrey and Smith had a legitimate expectation of privacy: "(1) whether the individual, by conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that he sought to preserve something as private; and (2) whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable."[191] The court had no trouble finding that Clements-Jeffrey and Smith expected their communications to stay private, noting their use of password protection and the intimate nature of the communications themselves.[192] However, the

reasonableness of the expectation depended on whether she should have known the laptop was stolen. The court found that there was a genuine issue of material fact as to whether Clements-Jeffrey should have known the laptop was stolen, and this precluded summary judgment.[193]

Clements-Jeffrey also argued that the police had violated her Fourth Amendment rights against unreasonable search and seizure by acquiring sexually explicit images that were unnecessary to their investigation and using them to humiliate her.[194] The court rejected this argument because the photographs were not the prodfuct of a police search, but were provided by Absolute.[195] The court similarly rejected Clements-Jeffrey's argument that the police had acted "in tandem" with Absolute in acquiring the photos, finding that there was no evidence that the police instigated, encouraged, or participated in the search performed by Absolute.[196]

As for the ECPA claims, Clements-Jeffrey and Smith argued that by disclosing and using the screenshots of their conversations, the police had violated 18 U.S.C. § 2511(1)(c) & (d), which prohibit the disclosure and use of illegally intercepted communications.[197] The court denied summary judgment to the police on these claims, rejecting their arguments that the disclosure and use of the screenshots were lawful.[198] The court further rejected the argument of the police that they had no reason to doubt the legality of Absolute's conduct, holding that a reasonable jury could conclude that the police should have known Absolute's actions were illegal.[199] The court also rejected the argument of the police that a "clean hands" exception previously recognized by the Sixth Circuit with respect to the exclusionary rule in criminal cases should apply to civil suits.[200] However, the court held that the officers were entitled to qualified immunity on the claims because the law in the area was not clearly established.[201]

Clements-Jeffrey and Smith also argued that Absolute violated 18 U.S.C. § 2511(1)(a) & (c) by intentionally intercepting their communications and disclosing them to the police.[202] Characterizing Clements-Jeffrey and Smith as "computer trespassers," Absolute countered that ECPA liability was precluded by 18 U.S.C. § 2511(2)(i), which provides generally that a person acting under color of law is not liable under the ECPA for intercepting the communications of a computer trespasser.[203] The court rejected this argument because Absolute was not acting under color of law.[204] Absolute argued further that "the rights of a user of stolen property can never trump the rights of the legal owner of the stolen property." The court rejected this argument because there was a question of fact about whether Clements-Jeffrey should have

known the computer was stolen.[205]

Clements-Jeffrey and Smith were allowed by the court to proceed against Absolute but not the police on their common-law invasion of privacy claims.[206] Ohio law recognizes a cause of action for "wrongful intrusion into one's private activities in such a way as to outrage or cause a person of ordinary sensibilities to suffer mental suffering, shame or humiliation."[207] The court held that a reasonable jury could find that Absolute's conduct met this standard.[208] However, the court held that the police could not be held liable for invading the plaintiffs' privacy because they were not involved in intercepting the screenshots.[209] Even though Clements-Jeffrey might have been humiliated by their use of the screenshots during Clements-Jeffrey's arrest, it did not do anything additional to invade her privacy.[210]

In sum, the court granted summary judgment on all claims against the police except for the Fourth Amendment claim relating to the warrantless search, about which the parties agreed that there were genuine issues of material fact.[211] However, the court denied summary judgment and allowed all of Clements-Jeffrey and Smith's claims to go forward against Absolute, a promising result for future victims of remote webcam activation and surveillance.[212] The case was ultimately settled.[213]

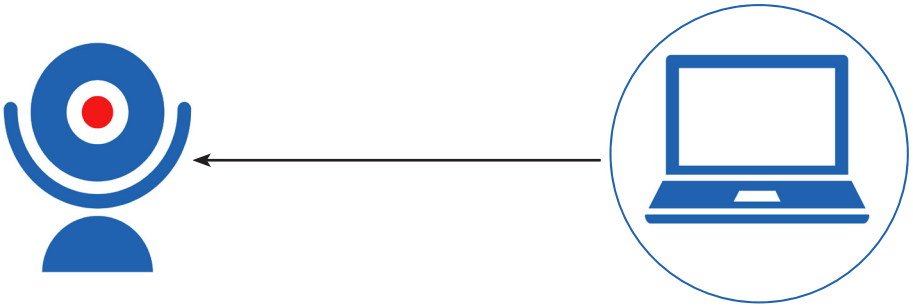
The Clements-Jeffrey case vividly illustrates the problems associated with the use of remote access tools by private companies to collect information for law enforcement. Absolute touts its investigation team, made up of "45 individuals with 1,000 years of combined experience in law enforcement."[214] Many join Absolute "after a full career in law enforcement," while others have backgrounds with "the FBI, the Marines, the US Army, Homeland Security and government positions."[215] Indeed, Absolute recruited Magnus, a longtime police officer, from his job with a sheriff's department.[216] The company states that its investigators "work closely with local police" to recover stolen devices.[217] According to a company datasheet, the company's investigators can:

- "Forensically mine a stolen or missing computer regardless of user or location
- Use key captures, registry and file scanning, geolocation, and other investigative techniques to understand how and why a device was breached
- Determine who has the computer, what they're doing with it, and whether any data was accessed. . . ."

While the company's current website remains silent on the issue of webcam activation, a 2010 report stated that the company's investigators retained the ability to do so.[218]

The court in Susan Clements-Jeffrey's case may have been too quick to find that Absolute was not acting as an agent of the police, instead finding that Absolute's theft recovery officer, Kyle Magnus, had simply introduced himself to the police after concluding his investigation and handed over the information he had gathered.[219] The evidence in the record on this point is ambiguous at best. Magnus testified that he did not recall sending screenshots to police officer Ashworth immediately after their first conversation, and Ashworth testified multiple times that he had "several conversations" and "many conversations" with Magnus in the course of the investigation.[220] Clements-Jeffrey testified in her deposition that Ashworth, after arresting her, told her, "We've had an officer in Milwaukee keeping you under surveillance over the last 16 days."[221] Contrary to the court's finding, the evidence suggests that Magnus and Absolute were effectively working on behalf of the Springfield police.

If this was the case, Clements-Jeffrey and Smith might have successfully pursued § 1983 claims against Absolute based on a state action theory. The state action doctrine holds that constitutional protections only bind the government and not private parties, except when private parties act as agents of the government.[222] Given the high potential for abuse by companies like Absolute, legislation is needed to prohibit this invasive alliance between police and private investigation. Such legislation would prevent bedrock constitutional rights from being nullified by private companies performing *de facto* police work.



7. LEGAL CONCERNS IN REMOTE ACTIVATION OF WEBCAMS BY INDIVIDUALS

Individuals have found a variety of innovative uses for webcams, such as to monitor their property or to keep an eye on their loved ones. Often, their purposes are benign. Using webcams remotely has helped people achieve ends as diverse as live streaming events and detecting cases of elder abuse by nursing home staff. Hidden,[223] an anti-theft app for Apple products, provides remote webcam activation capabilities similar to those previously offered by LANrev and PC Rental Agent. Hidden assisted in a well-publicized recovery of a stolen laptop; after the police declined to investigate the theft, the laptop's owner started a Tumblr blog and created Twitter posts containing webcam photos taken using Hidden of the man in possession of the laptop, who was soon identified.[224] Other tools such as GoToMyPC[225] offer similar functionality.[226]

But by providing for the remote activation of webcams, apps like Hidden and GoToMyPC raise the same concerns about potential invasion of privacy as tools like LANrev and PC Rental Agent. Like some government entities and private companies, individuals have sought to remotely activate others' webcams for questionable ends. Individuals are subject to the same hacking, wiretapping, and privacy laws as private companies and face the same criminal and civil liability for remotely activating webcams to breach others' privacy. However, to a greater extent than with companies, individuals who spy on others through their webcams may be "judgment-proof" and have no assets to provide for recovery in a civil action. Moreover, it is often difficult to discover the identity of the spying individual, absent a slip-up or voluntary self-disclosure.[227]

Even common video chat applications allowing remote webcam activation pose serious risks. In September 2010, Dharun Ravi, a first-year student at Rutgers Uni-

versity, and a friend, Molly Wei, accessed Ravi's webcam through Apple's iChat application from Wei's room down the hall, and briefly viewed his roommate, Tyler Clementi, kissing a man in the room Clementi shared with Ravi.[228] Ravi posted about the incident on Twitter ("Roommate asked for the room till midnight. I went to molly's room and turned on my webcam. I saw him making out with a dude. Yay."), and Clementi saw his Tweet.[229] Two days later, Clementi asked Ravi for private use of the room again for another romantic encounter and Ravi agreed. Later, Ravi publicized the encounter on Twitter in an apparent attempt to solicit viewers: "Anyone with iChat, I dare you to video chat me between the hours of 9:30 and 12. Yes, it's happening again."[230] Clementi saw the Tweet and turned off Ravi's computer prior to the encounter. The following evening, Clementi killed himself by jumping off the George Washington Bridge.[231]

Prosecutors declined to charge Ravi in connection with Clementi's death; he could also not be charged with wiretapping or unauthorized access to a computer, as the computer and room he videotaped were his.[232] Ravi was, however, charged and convicted of invasion of privacy as well as bias intimidation, tampering with a witness (by trying to influence what a witness told the police) and tampering with evidence (by deleting Tweets and posting a false Tweet).[233] Ravi was sentenced to 30 days in jail, three years of probation, 300 hours of community service and a $10,000 fine.[234]

Webcams have given rise to a disturbing practice known as "ratting," or installing a remote access Trojan on a victim's computer that can enable full control of the computer, including its webcam.

The widespread use of webcams has also given rise to a disturbing practice known as "ratting," or installing a remote access Trojan[235] on a victim's computer that can enable full control of the computer, including its webcam.[236] Ratters obtain images or video from their "slaves" by surreptitiously activating their webcams or combing through the contents of their hard drives. They then use the images or video for entertainment or to extort money or additional images or video of a sexual nature.[237]

While many ratters escape prosecution, law enforcement is increasingly paying attention to the phenomenon and has made some noteworthy arrests.[238] Luis Mijangos was arrested after using remote access Trojans to infect 129 computers, netting hundreds of victims.[239] The FBI "found different kinds of malware on [Mijangos'] computers [including] software to turn on webcams and microphones attached to

infected computers, and 'dozens of videos' from those webcams," most showing the victims getting out of the shower, dressing, or having sex.[240] Mijangos spread his malware by uploading it disguised as a popular song to a peer-to-peer file sharing network, and used it to take control of the computer of whomever downloaded the file. He would frequently reveal himself to a female victim as a hacker with control over her computer, telling her that he had seen an email she had just sent or heard a call she had just made, and demanding nude photos or video. If he gained control of a man's computer, he would send messages posing as the man to solicit nude photos from the man's girlfriend.

Mijangos' victims were traumatized. One victim, an underage woman from whom Mijangos extorted nude photos, moved away from her home near Los Angeles because of the incident; as she described the experience, "For the longest time I didn't know who this man was, why he was doing it or [if] he would come back. Not knowing is the worst, most dreaded feeling. It's always in the back of your mind. I moved away from the LA/OC [Los Angeles/Orange County] area but even here the thoughts never left me."[241] Mijangos ultimately pled guilty to felony wiretapping and computer hacking charges, and was sentenced to six years in prison.[242]

Prior to becoming Miss Teen USA 2013, Cassidy Wolf was the victim of another RAT-wielding "sextortionist."[243] Jared James Abrahams, a computer science student and former high school classmate of Wolf's, used a RAT to gain control of Wolf's computer and snap nude photos of her through her webcam, threatening to post them publicly unless she gave in to his demands.[244] He took control of Wolf's computer and changed the passwords on her Twitter, Tumblr, and email accounts. He then emailed Wolf, attaching nude pictures taken with her webcam, and writing:

> Here's what's going to happen! Either you do one of the things listed below or I upload these pics and a lot more (I have a LOT more and those are better quality) on all your accounts for everybody to see and your dream of being a model will be transformed into a pornstar. Do one of the following and I will give you back all your accounts and delete the pictures.
>
> 1) Send me good quality pics on Snapchat
>
> 2) Make me a good quality video
>
> 3) Go on skype with me and do what I tell you to do for 5 minutes
>
> If you don't do those or if you simply ignore this then those pics are

> going up all over the internet. It's your choice :) Also I'm tracking this email so I'll know when you open it. If you don't respond then your pics are going up.[245]

Instead, Wolf went to the FBI, which ultimately identified Abrahams as the culprit.[246] Abrahams later told the FBI that he had used a RAT to gain control over the laptops of up to 150 victims.[247] Wolf used her fame as Miss Teen USA to become an advocate for cybercrime awareness.[248] Abrahams pled guilty to federal computer hacking and extortion charges and was sentenced to 18 months in prison.[249]

Law enforcement authorities worldwide are turning increasing attention to the problem of ratters, as shown in May 2014, when raids in over a dozen countries led to the arrests of approximately 100 purchasers and users of Blackshades, a popular RAT that enabled spying through victims' computers.[250] Blackshades was created to be easy to use; according to computer security journalist Brian Krebs, it was "created and marketed principally for buyers who wouldn't know how to hack their way out of a paper bag."[251] Blackshades sold for as little as $40 online, and could provide a ratter with full control over a victim's computer, including the ability to capture screenshots, log keystrokes, control access to files, and activate the webcam.[252] Gaining access to, or "infecting," a victim's computer involved tricking the owner into clicking a malicious web link or opening a corrupted file.[253] According to the FBI, Blackshades was "used to infect more than half a million computers worldwide."[254] Blackshades was ratter Jared James Abrahams' tool of choice in his snooping and attempted extortion of Cassidy Wolf.[255] While owning Blackshades is not in itself illegal, surreptitiously installing it on a victim's computer is considered computer hacking crime in many countries.[256]

One ratter spread his malware by disguising it as a popular song on a peer-to-peer sharing network, taking control of the computer of anyone who downloaded the song.

In November 2014, law enforcement authorities in Europe arrested ratters in the United Kingdom, Estonia, France, Italy, Latvia, Norway and Romania. British cybercrime investigator Peter Goodman stated, "The response on this occasion has been enforcement action … to strike a blow against a particularly pernicious and invasive form of cyber-criminality"—ratters who can turn on victims' webcams and access banking or personal information.[257]

Ratters in the United States can be criminally charged under the federal Computer Fraud and Abuse Act for illegally accessing their victims' computers. However, their victims generally cannot sue them in civil court under the CFAA because

of the civil suit requirement of proof of monetary damages of over $5,000. In contrast, certain states' computer trespass laws do allow civil suits by victims for unauthorized computer access without a monetary harm requirement.[258]

8. POLICY RECOMMENDATIONS

Webcams present the opportunity for countless innovative uses by governments, businesses, and individuals. They have permanently changed the way we connect across distances with friends, family, and even employers, colleagues, and doctors. They entertain us and make us more productive. But policymakers have directed too little attention to how the ubiquity of webcams has infringed our privacy. Governments, businesses, and individuals have all taken advantage of the spread of webcams to surveil us in shocking ways.

The ability to activate webcams remotely has garnered relatively little attention from lawmakers or policy analysts. Efforts to reform government surveillance have focused primarily on the bulk telephony metadata collection program under Section 215 of the PATRIOT Act program which does not involve hacking computers or targeting webcam transmissions. On the legislative front, U.S. Senators Ron Wyden, Mark Udall, and Martin Heinrich have called for an investigation into the National Security Agency (NSA)'s role in assisting with the U.K.'s Government Communications Headquarters (GCHQ) with its global webcam chat surveillance program, Optic Nerve.[259] Independent advocacy groups including the Electronic Frontier Foundation (EFF) and American Civil Liberties Union (ACLU) have criticized the role of secret courts and gag orders in enabling electronic surveillance.[260]

In response to the Lower Merion case, the state of New Jersey passed the "Anti-Big Brother Act." That law requires school districts that provide students with devices including cameras or tracking technologies to notify them "that the electronic device may record or collect information on the student's activity or the student's use of the device."[261] The notice must also state that the district "shall not use any of the capabilities in a manner that would violate the privacy rights of the student or any

individual residing with the student."[262] School districts are required to gather an acknowledgement of receipt of the notice from a parent or guardian on an accompanying form and to retain the form for as long as the student has the device.[263] At the national level, late U.S. Senator Arlen Specter proposed the Surreptitious Video Surveillance Act of 2010, an amendment to the ECPA, to explicitly prohibit silent video interceptions without prior court approval, but the bill died in committee.[264]

We need stronger laws and regulations to protect our right to privacy as we move forward into the interconnected age. We recommend the following policy changes:

Policymakers have directed too little attention to how the abuses of webcams have negatively impacted privacy.

The government should be prohibited from using remote webcam activation in criminal investigations. The use of a webcam to invade someone's home to collect evidence is in direct contradiction of fundamental values under the U.S. Constitution. By targeting a webcam rather than a particular user, remote activation is likely to invade the privacy of third parties. Video surveillance is uniquely intrusive under any circumstances because a webcam is typically located in the home, where our notions of privacy are strongest.[265] Allowing law enforcement to remotely activate webcams is akin to giving the government a pair of eyes in every home—something the Founders prohibited in the Third Amendment, which prohibits the quartering of soldiers without the owner's consent, except in a manner prescribed by law.[266] Additionally, webcam use by government investigators is an unreasonable search under the Fourth Amendment.

The proposed changes to Rule 41(b) that significantly narrow the territoriality requirement should be rejected. While the government asserts a valid interest in being able to coordinate searches across jurisdictions in limited situations, such as to investigate a botnet, it should not be permitted largely to do away with the territoriality requirement altogether in cases of suspected computer crimes, as the proposed changes would. As reflected in the Third Circuit's recent reversal of a CFAA conviction on venue grounds, territoriality matters, even in the internet age.[267]

As for private businesses, the documented cases of remote webcam activation on record counsel strongly for laws banning their use of the technology outright. **Private businesses should be prohibited from remotely activating users' webcams, because their doing so poses extraordinary threats to users'**

privacy that the actual or perceived benefits do not come close to balancing. As reflected in testimony in the Byrds' lawsuit over PC Rental Agent, remotely activating the webcam on a computer reported stolen is not required to locate the computer. Congress should pass legislation criminalizing the remote activation of another person's webcam,[268] and should forbid rental companies or other companies from activating the computer webcam on users of their computers. A company like Absolute Software should not be permitted to offer customers a *de facto* private police force that exists for the purpose of performing highly invasive searches outside the reach of constitutional protections.

Additionally, greater efforts should be made to curb the abusive actions of malicious individual ratters, even those who do not target a large number of victims or an unusually high-profile victim. Any ratter who accesses another's computer without authorization violates a number of privacy and computer crime laws, and any extortion or attempt to extort a victim using information gathered is an additional state and federal crime. The damage malicious ratters can do to their victims is extreme, in emotional and sometimes in monetary terms. Whether through increased training and resources to law enforcement in this area, or through the passage of laws specifically targeting the practice, additional measures should be taken to ensure that malicious ratters cannot continue to inflict emotional distress and to extort their victims with impunity. More states should pass laws allowing civil suits by victims for unauthorized access to their computers without any requirements of proof of monetary damages. Law enforcement and the judicial system should step up their efforts to prevent, investigate, and punish anyone who criminally invades computer users' privacy.

NOTES

1 Skype, http://www.skype.com/en/.

2 Tiffiny Carlson, "8 Innovative and Fun Ways to Use Your Webcam," *TechNorms*, September 17, 2013, http://www.technorms.com/33978/innovative-and-fun-ways-to-use-your-webcam.

3 *Id.*

4 Josh Silverman, "Granny Cam - Surveillance in Nursing Homes," July 2, 2013, http://www.joshsilvermanlaw.com/blog/2013/07/02/granny-cam-surveillance-in-nursing-131232.

5 Milt Freudenheim, "The Doctor Will See You Now. Please Log On." *The New York Times*, May 30, 2010, at BU1.

6 Tiffiny Carlson, "8 Innovative and Fun Ways to Use Your Webcam," *TechNorms*, September 17, 2013, http://www.technorms.com/33978/innovative-and-fun-ways-to-use-your-webcam.

7 *Id.*

8 YouTube, "Statistics," https://www.youtube.com/yt/press/statistics.html.

9 Brian Stelter, "Addictive Animal Webcams Get Network Attention," *The New York Times*, April 3, 2013, at B1.

10 Vikas Bajaj, "Transparent Government, via Webcams in India," *The New York Times*, July 18, 2011, at B3.

11 Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "You Only Click Twice: FinFisher's Global Proliferation," CitizenLab, (Mar. 13, 2013), https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/; Vernon Silver, "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma," *Bloomberg*, July 25, 2012, http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html.

12 Craig Timberg and Ellen Nakashima, "FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance," *Washington Post,* December 6, 2013, http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story_3.html.

13 *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753 (S.D. Tex. Apr. 22, 2013)

14 Ballard Spahr, "Report of Independent Investigation: Regarding Remote Monitoring of Student Laptop Computers by the Lower Merion School District," May 3, 2010, at 2.

15 The acronym RAT in this context can stand for either Remote Administration Tool or Remote Access Trojan. The two terms appear to be used interchangeably. *See, e.g.*, Mary Landesman, "Remote Access Trojan," *About.com*, http://antivirus.about.com/od/whatisavirus/g/rat.htm; Margaret Rouse, "What is a RAT (Remote Access Trojan)?" *TechTarget*, http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan. "Remote Access Trojan" is used here because the term more clearly connotes the user's intent to gain unauthorized access to a computer.

16 Nate Anderson, "Meet the Men Who Spy on Women Through Their Webcams," *Ars Technica*, March 10, 2013, http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/.

17 *See, e.g.*, Claire Cain Miller, "Tech's Man Problem," *The New York Times*, April 6, 2014, at BU1;

Amanda Hess, "Why Women Aren't Welcome on the Internet," *Pacific Standard*, January 6, 2014, http://www.psmag.com/navigation/health-and-behavior/women-arent-welcome-internet-72170/.

18 Nate Anderson, "Meet the Men Who Spy on Women Through Their Webcams," *Ars Technica*, March 10, 2013, http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/.

19 *Id.*

20 Jay Novak, Jonathan Stribley, Kenneth Meagher, and J. Alex Halderman, "Absolute Pwnage: A Short Paper About the Security Risks of Remote Administration Tools," Proc. 15th Annual Financial Cryptography Conference (Jan. 2011), https://jhalderm.com/pub/papers/pwnage-fc11.pdf. For an illustration of the abundance of legitimate remote administration software, see Wikipedia, "Comparison of Remote Desktop Software," http://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software (last modified May 31, 2014).

21 Whitson Gordon, "Use Your Computer From Anywhere: A Guide to Remote Controlling Your PC," Lifehacker, (Jan. 24, 2014), http://lifehacker.com/5902654/use-your-home-computer-from-anywhere-a-comprehensive-guide-to-remote-controlling-your-pc.

22 Dave Shackleford, "Compliance and Security Challenges With Remote Administration," SANS Institute, http://www.sans.org/reading-room/whitepapers/analyst/compliance-security-challenges-remote-administration-34945; Absolute Software, http://lojack.absolute.com/en.

23 *See, e.g.*, http://www.pcrentalagent.com/eSiteWay/Home.aspx.

24 Kashmir Hill, "Thousands Of People Oblivious To Fact That Anyone On The Internet Can Access Their Computers," *Forbes.com*, August 13, 2014, http://www.forbes.com/sites/kashmirhill/2014/08/13/so-many-pwns/.

25 Jody Avirgan, "A Running List of What We Know the NSA Can Do. So Far." WNYC, (Jan. 17, 2014), http://www.wnyc.org/story/running-list-what-we-know-nsa-can-do-so-far/. The Five Eyes countries are the United States, United Kingdom, Australia, Canada, and New Zealand. Martin Asser, "Echelon: Big Brother Without a Cause?" *BBC News*, July 6, 2000, http://news.bbc.co.uk/2/hi/europe/820758.stm.

26 *American Civil Liberties Union v. Clapper*, 959 F.Supp.2d 724, 733-34 (S.D.N.Y. 2013). The data collected includes "the telephone numbers that placed and received the call, the date, time, and duration of the call, other session-identifying information (for example, International Mobile Subscriber Identity number, International Mobile station Equipment Identity number, et cetera), trunk identifier, and any telephone calling card number." *Id.*

27 Spencer Ackerman and James Ball, "Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ," *The Guardian*, February 27, 2014, http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

28 50 U.S.C. §§ 1801 *et seq*.

29 Stephen William Smith, "Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket," 6 *Harvard Law & Policy Review* 313, 323 (2012), http://www3.law.harvard.edu/journals/hlpr/files/2013/06/Gagged-Sealed-and-Delivered.pdf.

30 *Id.* at 315.

31 Jacqui Cheng, "Report Blames IT for Bad Procedures in School 'Spying' Case," *Ars Technica*, May 6, 2010, http://arstechnica.com/tech-policy/2010/05/report-blames-it-for-bad-procedures-in-school-spying-case/. Following a lawsuit, Absolute removed LANrev's

Theft Track feature, which provided the screenshot and webcam activation capabilities to customers; however, its internal team of investigators appears to retain webcam activation capabilities. Bill Detweiler, "LANrev to Lose Theft Track Feature Following Pa. School Spying Allegations," *Tech Republic*, February 23, 2010, http://www.techrepublic.com/blog/tr-dojo/lanrev-to-lose-theft-track-feature-following-pa-school-spying-allegations/.

32 Lori Andrews, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* 111 (New York: Free Press 2011).

33 *Id.*

34 *Id.* at 112.

35 *Id.*

36 *Id.*

37 *Id.* at 133.

38 *Id.* at 115.

39 *Id.* at 113.

40 *Id.*

41 Martha Neil, "7 Retailers Settle with FTC, Agree to Stop Spying on Up to 400,000 Computer Rental Customers," *ABA Journal*, September 26, 2012, http://www.abajournal.com/news/article/7_Companies_Settle_With_FTC_Agree_to_Stop_Using_Rental_Computer_Webcams_to/.

42 Julianne Pepitone, "'Creepware' Hacker Sting Nets 97 Worldwide," *NBC News*, May 19, 2014, http://www.nbcnews.com/tech/security/creepware-hacker-sting-nets-97-worldwide-n109061.

43 Nate Anderson, "Meet the Men Who Spy on Women Through Their Webcams," *Ars Technica*, March 10, 2013, http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/.

44 Nate Anderson, "How an Omniscient Internet 'Sextortionist' Ruined the Lives of Teen Girls," *Ars Technica*, September 7, 2011, http://arstechnica.com/tech-policy/2011/09/how-an-omniscient-internet-sextortionist-ruined-lives/.

45 Nate Anderson, "How the FBI Found Miss Teen USA's Webcam Spy," *Ars Technica*, September 27, 2013, http://arstechnica.com/tech-policy/2013/09/miss-teen-usas-webcam-spy-called-himself-cutefuzzypuppy/.

46 Federal Bureau of Investigation, "International Blackshades Malware Takedown: Coordinated Law Enforcement Actions Announced," May 19, 2014, http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/.

47 FinFisher, http://www.finfisher.com/FinFisher/index.html.

48 Fahmida Y. Rashid, "FinFisher Spyware C&C Server Detected in US," *PC Magazine*, August 8, 2012, http://securitywatch.pcmag.com/none/301324-finfisher-spyware-c-c-server-detected-in-us.

49 Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola, "Police Story: Hacking Team's Government Surveillance Malware," Citizen Lab, (June 24, 2014), https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/.

50 Morgan Marquis-Boire, "Schrodinger's Cat Video and the Death of Clear-Text," Citizen Lab, (Aug. 15, 2014), https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/; Morgan Marquis-Boire, "You Can Get Hacked Just By Watching This Cat Video on YouTube," *The Intercept*, August 15, 2014, https://firstlook.org/theintercept/2014/08/15/cat-video-hack/.

51 Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola, "Police Story: Hacking Team's Government Surveillance Malware," Citizen Lab, (June 24, 2014), https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/; Vernon Silver, "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma," *Bloomberg*, July 25, 2012, http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html.

52 Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "You Only Click Twice: FinFisher's Global Proliferation," CitizenLab, (Mar. 13, 2013), https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/; The full list of countries was: Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, and Vietnam.

53 Nate Anderson, "Meet the Men Who Spy on Women Through Their Webcams," *Ars Technica*, March 10, 2013, http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/.

54 *Id.*

55 *Id.*

56 *Id*; *see also* Paul Ohm, "The Myth of the Superuser: Fear, Risk, and Harm Online," 41 *UC Davis L. Rev.* 1327, 1367-70 (Apr. 2008) (discussing Kevin Mitnick and debunking popular conception of the "hacker" as possessing extraordinary powers).

57 Ian Parker, "The Story of a Suicide," *The New Yorker*, February 6, 2012, http://www.newyorker.com/reporting/2012/02/06/120206fa_fact_parker.

58 Ashkan Soltani and Timothy B. Lee, "Research Shows How MacBook Webcams Can Spy on Their Users Without Warning," *Washington Post*, December 18, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/18/research-shows-how-macbook-webcams-can-spy-on-their-users-without-warning/

59 *See, e.g.*, "Can Webcams be Turned on Without the Indicator Light?," *Stackexchange.com*, http://security.stackexchange.com/questions/6758/can-webcams-be-turned-on-without-the-indicator-light.

60 *See* Craig Timberg and Ellen Nakashima, "FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance," *Washington Post,* December 6, 2013, http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story_3.html.

61 Ashkan Soltani and Timothy B. Lee, "Research Shows How MacBook Webcams Can Spy on Their Users Without Warning," *Washington Post*, December 18, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/18/research-shows-how-macbook-webcams-can-spy-on-their-users-without-warning/.

62 U.S. Const. Am. IV.

63 *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. , concurring).

64 *United States v. Koyomejian*, 970 F.2d 536, 551 (9th Cir. 1992) (*en banc*) (Kozinski, J. , concurring in the judgment).

65 *LaLonde v. County of Riverside*, 204 F.3d 947, 954 (9th Cir. 2000) (citing *United States v. Winsor*,

846 F.2d 1569, 1577-1578 (9th Cir.1988) (*en banc*)).

66 Section 1830(a)(2)(C), CFAA's broadest provision, prohibits obtaining information via unauthorized, intentional access of a "protected computer," which in practice means most computers. *See* Orin S. Kerr, *Computer Crime Law* 29, 561 (St. Paul, MN: West, 2009).

67 *United States v. Nosal*, 2013 WL 5434054 (N.D. Cal. Apr. 19, 2013); *United States v. Auernheimer*, 2012 WL 5389142 (D.N.J. Oct. 26, 2012), *rev'd on venue ground*, 748 F.3d 525 (3d Cir. 2014).

68 18 U.S.C. § 1030(c)(4)(A)(i)(I).

69 *See, e.g.*, Transcript and Order from Hearing on Objections to the Magistrate Judge's Report and Recommendation, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Apr. 24, 2012), ECF No. 96, p. 49.

70 *United States v. Steiger*, 318 F.3d 1039, 1048-1050 (11th Cir. 2003).

71 Transcript and Order from Hearing on Objections to the Magistrate Judge's Report and Recommendation, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Apr. 24, 2012), ECF No. 96, p. 49.

72 Decision and Order, *In the Matter of Aaron's, Inc.*, Federal Trade Commission, File No. 1123264 (Mar. 11, 2014); Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013).

73 Decision and Order, *In the Matter of Aaron's, Inc.*, Federal Trade Commission, File No. 1123264 (Mar. 11, 2014); Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013).

74 *See, e.g.*, *Clements-Jeffrey v. City of Springfield*, 810 F.Supp.2d 857 (S.D. Ohio 2011); Megan DeMarco, "Live Coverage: Dharun Ravi Found Guilty on Most Counts in Webcam Spying Trial Verdict," *NJ.com*, March 16, 2012, http://www.nj.com/news/index.ssf/2012/03/ravi_webcam_trial_verdict.html.

75 In October 2014, Aaron's, Inc. and their franchises settled a lawsuit filed by the California Attorney General's office in the Superior Court for the County of Los Angles, case number BC559774, which, among other things, accused Aaron's, Inc. of violating the privacy rights of California citizens. Article 1, Section 1 of the California State Constitution that states people have an inalienable right to privacy. The Attorney General's office alleged that the "detective mode" of PC Rental Agent could activate webcams and microphones to monitor people without their knowledge thus invading the privacy of citizens of California by covertly colleting their personal information. While Aaron's, Inc. admitted no wrongdoing, it agreed to settle the case for $28.4 million including $3.4 million in civil damages and fines with the remaining $25 million to go to customers whose privacy may have been affected. Associated Press, "Rent-To-Own Business Aaron's, Inc. To Pay 28.4M To Settle Privacy Lawsuit," *Cbslocal.com* (Los Angeles), October 13, 2014, http://losangeles.cbslocal.com/2014/10/13/rent-to-own-business-aarons-to-pay-28-4m-to-settle-privacy-lawsuit/.

76 *See, e.g.*, Ark. Code Ann. § 5-41-104(a); Ark. Code Ann. § 5-41-106; Cal. Penal Code Ann. § 502(c)(7); Cal. Penal Code Ann. § 502(e)(1); Del. Code Ann. tit. 11, § 932; Del. Code Ann. tit. 11, § 941; Fla. Stat. Ann. § 815.06(1)(a); Fla. Stat. Ann. § 815.06(5)(a); 720 Ill. Comp. Stat. Ann. 5/17-51(a)(1); 720 Ill. Comp. Stat. Ann. 5/17-51(c); Iowa Code Ann. § 716.6B(1)(c); Iowa Code Ann. § 716.6B(2); Mo. Ann. Stat. § 569.099(1)(1); Mo. Ann. Stat. § 537.525(1); Nev. Rev. Stat. Ann. § 205.4765(3)(k); Nev. Rev. Stat. Ann. § 205.511; N.J. Stat. Ann. § 2C:20-25(a); N.J. Stat. Ann. § 2A:38A-3(c); N.C. Gen. Stat. Ann. § 14-454(b); N.C. Gen. Stat. Ann. § 14-458(c); N.D. Cent. Code Ann. § 12.1-06.1-08(2); N.D. Cent. Code Ann. § 12.1-06.1-08(3); Okla. Stat. Ann. tit. 21, § 1953(A)

(4); Okla. Stat. Ann. tit. 21, § 1955(C); R.I. Gen. Laws § 11-52-3; R.I. Gen. Laws § 11-52-6; Tenn. Code Ann. § 39-14-602(b)(1); Tenn. Code Ann. § 39-14-604(a); Vt. Stat. Ann. tit. 13, § 4102; Vt. Stat. Ann. tit. 13, § 4106; W. Va. Code Ann. § 61-3C-5; W. Va. Code Ann. § 61-3C-16.

77 U.S. Const. Am. IV.

78 *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753 at 759-760 (S.D. Tex. Apr. 22, 2013) (citing *United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987)).

79 18 U.S.C. §§ 2516-2518.

80 In the federal court system, magistrate judges are appointed by federal district judges pursuant to the Federal Magistrates Act of 1968, 28 U.S.C. § 631 *et seq.*, and typically handle discovery and other pretrial matters.

81 *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753 (S.D. Tex. Apr. 22, 2013).

82 *Id.* at 757-758. (citing Fed. R. Crim. P. 41(b)).

83 *Id.* at 758-759.

84 *Id.* at 759-760. (citing *United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987)).

85 *Id.* at 755.

86 *Id.*

87 *Id.* at 755-756.

88 *Id.* at 756-758.

89 *Id.* at 756.

90 *Id.*

91 *Id.* at 757.

92 *Id.*

93 *Id*.

94 *Id.* at 756-757.

95 *Id.* at 758. (quoting U.S. Const. Am. IV).

96 *Id.* at 759.

97 *Id.*

98 *Id.* (brackets in original).

99 *Id.*

100 *United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987).

101 *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753 at 759-760 (S.D. Tex. Apr. 22, 2013) (discussing *United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987)) (citations omitted).

102 *Id.* at 760. (citing *United States v. Cuevas-Sanchez*, 821 F.2d 248, 252 (5th Cir. 1987)).

103 *Id.*

104 *Id.*

105 *Id.*

106 *Id.* (citing *United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987) ("A juxtaposition of such contentions trifles with the Court.")).

107 *Id.*

108 *Id.*

109 Letter from U.S. Department of Justice to Hon. Reena Raggi, September 18, 2013, http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/cr-suggestions-2013/13-CR-B-Suggestion_Raman.pdf.

110 *Id.*

111 Agenda Book, Standing Committee on Rules of Practice and Procedure, Washington, DC, May 29-30, 2014, http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Standing/ST2014-05.pdf.

112 Memorandum from American Civil Liberties Union to Members of the Advisory Committee on Criminal Rules, April 4, 2014, at 7, https://www.aclu.org/sites/default/files/assets/aclu_comments_on_rule_41.pdf.

113 *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753 at 760 (S.D. Tex. Apr. 22, 2013) (citing *United States v. Cuevas-Sanchez*, 821 F.2d 248, 252 (5th Cir. 1987)).

114 Absolute Software, "Recovery Statistics," http://www3.absolute.com/support/consumer/recovery_statistics.

115 *See* Comment of Timothy Kelly (DesignerWare) on Proposed Consent Agreement *In the Matter of DesignerWare, LLC*, FTC File No. 1123151 #00016, http://www.ftc.gov/policy/public-comments/comment-00016-7 (claiming that Detective Mode was installed only when a rental customer reported a computer stolen, in which event "the owner of the computer [n.b. , the rent-to-own store – *compare generally* Testimony of Timothy Kelly, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. May 26, 2011), ECF No. 41] could ask to have an additional program installed called the Detective Mode Program which would gather information to prove whether or not the renter that claimed it was stolen was still using it"). Kelly, in addition to co-owning Aaron's franchise stores, created PC Rental Agent. *Id.*

116 18 U.S.C. § 1030(c)(4)(A)(i)(I).

117 18 U.S.C. §§ 2511, 2520.

118 Transcript and Order from Hearing on Objections to the Magistrate Judge's Report and Recommendation, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Apr. 24, 2012), ECF No. 96, p. 49.

119 "Invasion of Privacy," *IT Law Wiki*, http://itlaw.wikia.com/wiki/Invasion_of_privacy (last updated Mar. 15, 2014) ("Only North Dakota and Wyoming have not yet recognized any of the four privacy torts.").

120 Cal. Const. , art. I, § 1; Without My Consent, "Cal. Const. , art. I, § 1," http://www.withoutmyconsent.org/attorneys/california-constitution-art-i-%C2%A7-1.

121 An exception is Wyoming, which has both no privacy statute and no common-law cause of action for invasion of privacy. *See* Order, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Jan. 27, 2014), ECF No. 318, pp. 28-31.

122 Anya Schiffrin, "Pay Now, Pay Later," *Mother Jones*, May/June 2005, http://www.motherjones.com/politics/2005/05/pay-now-pay-later.

123 Eligio Pimentel, "Renting-to-Own: Exploitation or Market Efficiency?" 13 *Law & Ineq.* 369, 370 (1994-1995).

124 Virginia Eubanks, "Want to Predict the Future of Surveillance? Ask Poor Communities." *The American Prospect*, January 15, 2014, http://prospect.org/article/want-predict-future-surveillance-ask-poor-communities; John Gilliom, *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy* (U. Chi. Press 2001).

125 Dan Goodin, "How Spyware on Rental PCs Captured Users' Most Intimate Moments," *Ars Technica*, December 18, 2012, http://arstechnica.com/security/2012/12/how-spyware-on-rental-pcs-captured-users-most-intimate-moments/.

126 *Id*; *see also* Plaintiffs' Exhibit 2 in Support of Motion for Preliminary Injunction, *Byrd*

v. Aaron's, Inc., No. 1:11-cv-00101 (W.D. Pa. May 25, 2011), ECF No. 40-2, p. 4. In a police interview about the incident, Christopher Mendoza, the Aspen Way employee who had confronted Brian Byrd with the photographs, "stated the accounts had been mixed up" and showed a different customer's account overdue with Crystal Byrd's computer as the item in question.

127 Dan Goodin, "How Spyware on Rental PCs Captured Users' Most Intimate Moments," *Ars Technica*, December 18, 2012, http://arstechnica.com/security/2012/12/how-spyware-on-rental-pcs-captured-users-most-intimate-moments/.

128 *Id.*

129 Plaintiffs' Exhibit 2 in Support of Motion for Preliminary Injunction, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. May 25, 2011), ECF No. 40-2, pp. 9-10.

130 Corrected Third Amended Class Action Complaint, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Oct. 2, 2013), ECF No. 296, p. 25.

131 Dan Goodin, "How Spyware on Rental PCs Captured Users' Most Intimate Moments," *Ars Technica*, December 18, 2012, http://arstechnica.com/security/2012/12/how-spyware-on-rental-pcs-captured-users-most-intimate-moments/.

132 Testimony of Timothy Kelly, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. May 26, 2011), ECF No. 41, p. 7.

133 Dara Kerr, "Aaron's Computer Rental Chain Settles FTC Spying Charges," *CNET*, October 22, 2013, http://news.cnet.com/8301-1009_3-57608838-83/aarons-computer-rental-chain-settles-ftc-spying-charges/.

134 Testimony of Timothy Kelly, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. May 26, 2011), ECF No. 41, pp. 48-52; Testimony of Chastity Hittinger, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. May 31, 2011), ECF No. 43, p. 116.

135 Testimony of Chastity Hittinger, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. May 31, 2011), ECF No. 43, p. 115.

136 *Id.* at 116.

137 Class Action Complaint, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. May 3, 2011), ECF No. 1, pp. 12-16.

138 *Id.* at 16-18.

139 Brief in Support of Defendant DesignerWare, LLC's Motion to Dismiss Pursuant to F.R.C.P. 12(b)(1) and 12(b)(6) Or, in the Alternative, Motion for Summary Judgment Pursuant to F.R.C.P. 56, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Jul. 13, 2011), ECF No. 63; Defendant Aaron's, Inc.'s Memorandum of Law in Support of its Motion to Dismiss Plaintiffs' First Amended Complaint, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Aug. 17, 2011), ECF No. 75. Separately, Aspen Way moved to dismiss based on lack of personal jurisdiction, an argument I will not address here. *See* Defendant Aspen Way Enterprises, Inc.'s Brief in Support of Its Motion to Dismiss the Amended Complaint, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Aug. 18, 2011), ECF No. 77.

140 Brief in Support of Defendant DesignerWare, LLC's Motion to Dismiss Pursuant to F.R.C.P. 12(b)(1) and 12(b)(6) Or, in the Alternative, Motion for Summary Judgment Pursuant to F.R.C.P. 56, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Jul. 13, 2011), ECF No. 63; Defendant Aaron's, Inc.'s Memorandum of Law in Support of its Motion to Dismiss Plaintiffs' First Amended Complaint, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Aug. 17, 2011), ECF No. 75.

141 The Byrds later dropped the Section 2511 and CFAA claims, and filed an amended complaint adding claims for common-law invasion of privacy. Defendant Aaron's, Inc.'s Memorandum of Law in Support of its Motion to Dismiss Plaintiffs' First Amended Complaint, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Aug. 17, 2011), ECF No. 75.

142 Defendant Aaron's, Inc.'s Memorandum of Law in Support of Its Motion to Dismiss Plaintiffs' Third Amended Complaint, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Jun. 11, 2013), ECF No. 164, pp. 13-14.

143 *Id.* at 12-15.

144 Transcript of Hearing, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. May 24, 2013), ECF No. 135, pp. 38-44.

145 Plaintiffs' Brief in Opposition to Defendant Aaron's, Inc.'s Motion to Dismiss Plaintiffs' Third Amended Complaint, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Jul. 1, 2013), ECF No. 173, pp. 3-9 (citing *Shefts v. Petrakis*, 10-CV-1104, 2012 WL 4049484 (C.D. Ill. Sept. 13, 2012) (holding that screenshots captured by similar remote administration software constituted contemporaneous interceptions)).

146 Magistrate Judge's Report and Recommendation, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Feb. 17, 2012), ECF No. 85, pp. 13-14 (citing *Brahmana v. Lembo*, 2009 WL 1424438 (N.D. Cal. May 20, 2009)).

147 *Id.* at 14.

148 Transcript and Order from Hearing on Objections to the Magistrate Judge's Report and Recommendation, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Apr. 24, 2012), ECF No. 96, p. 49.

149 Orders, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Mar. 31, 2014), ECF Nos. 339 & 340.

150 *See* Order, *Byrd v. Aaron's, Inc.*, No. 1:11-cv-00101 (W.D. Pa. Mar. 31, 2014), ECF No. 339, p. 4 (highlighting the parties' disagreement over whether an "interception" had occurred and expressing judicial doubt but allowing the Byrds' ECPA claim to survive motion to dismiss).

151 Complaint, *Peterson v. Aaron's, Inc.*, No. 1:14-mi-99999-UNA (N.D. Ga. June 19, 2014); *see also* America Now, "Herman Gerel LLP: Aaron's Inc. Faces More Computer Spyware Allegations," June 19, 2014, http://www.americanownews.com/story/25821689/herman-gerel-llp-aarons-inc-faces-more-computer-spyware-allegations.

152 15 U.S.C § 45(a)(1).

153 15 U.S.C § 45(n).

154 *Federal Trade Commission v. Wyndham Worldwide Corp.*, 10 F.Supp.3d. 602 (D. N.J. Apr. 7, 2014).

155 Federal Trade Commission, "FTC Halts Computer Spying," September 25, 2012, http://www.ftc.gov/news-events/press-releases/2012/09/ftc-halts-computer-spying; Federal Trade Commission, "Aaron's Rent-To-Own Chain Settles FTC Charges That it Enabled Computer Spying by Franchisees," October 22, 2013, http://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer.

156 Complaint, *In the Matter of Aaron's, Inc.*, Federal Trade Commission, File No. 1123264 (Oct. 22, 2013); Complaint, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, Docket No. C-4392 (Sept. 25, 2012); Complaint, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Sept. 25, 2012).

157 Complaint, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, Docket No. C-4392 (Sept. 25, 2012), pp. 1-2.

158 *Id*. at 2-3.

159 Complaint, *In the Matter of Aaron's, Inc.*, Federal Trade Commission, File No. 1123264 (Oct. 22, 2013); Complaint, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Sept. 25, 2012).

160 Complaint, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, Docket No. C-4392 (Sept. 25, 2012), p. 3.

161 *Id.*

162 Complaint, *In the Matter of Aaron's, Inc.*, Federal Trade Commission, File No. 1123264 (Oct. 22, 2013), p. 1.

163 *Id.*

164 *Id.* at 3.

165 *Id.* at 2.

166 *Id.*

167 Decision and Order, *In the Matter of Aaron's, Inc.*, Federal Trade Commission, File No. 1223264 (Mar. 11, 2014); Decision and Order, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Apr. 15, 2013); Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013).

168 The orders define "monitoring technology" as "any hardware, software, or application utilized in conjunction with a computer that can cause the computer to (1) capture, monitor, or record, and (2) report information about user activities by: (a) Recording keystrokes, clicks, or other user-generated actions; (b) Capturing screenshots of the information displayed on a computer monitor or screen; or (c) Activating the camera or microphone function of a computer to take photographs or record audio or visual content through the computer's webcam or microphone." Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013), p. 3; Decision and Order, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Apr. 15, 2013), p. 3.

169 Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013), pp. 3-4; Decision and Order, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Apr. 15, 2013), pp. 3-4.

170 *Id.*

171 "Geophysical location tracking technology" is defined as "any hardware, software, or application utilized in conjunction with a computer that collects and reports data or information that identifies the precise geophysical location of the computer[,]" including "technologies that report: the GPS coordinates of a computer; theWiFi signals available to or actually used by a computer to access the Internet; the telecommunication towers or connections available to or actually used by a computer; [or] the processing of any such reported data through geolocation lookup services[.]" Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013), p. 3; Decision and Order, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Apr. 15, 2013), p. 3.

172 Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013), p. 4; Decision and Order, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Apr. 15, 2013), p. 4.

173 Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013), p. 5; Decision and Order, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Apr. 15, 2013), p. 5. In this event, the company is required

to retain records of a theft being reported and a police report being filed.

174 Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013), p. 5; Decision and Order, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Apr. 15, 2013), p. 5.

175 Decision and Order, *In the Matter of Aspen Way Enterprises, Inc.*, Federal Trade Commission, File No. 1123151 (Apr. 11, 2013), p. 5; Decision and Order, *In the Matter of DesignerWare, LLC*, Federal Trade Commission, File No. 1123151 (Apr. 15, 2013), p. 5.

176 Decision and Order, *In the Matter of Aaron's, Inc.*, Federal Trade Commission, File No. 1223264 (Mar. 11, 2014), pp. 7-8.

177 *Walter v. U.S.*, 447 U.S. 649, 662 (1980) (Blackmun, J. , dissenting).

178 *Clements-Jeffrey v. City of Springfield*, 810 F.Supp.2d 857, 868-869 (S.D. Ohio 2011) (citations omitted).

179 *Id.* at 860.

180 *Id.* at 861.

181 *Id.* at 861-862.

182 *Id.*

183 *Id.* at 862.

184 *Id.* at 862-863.

185 *Id.*

186 *Id.* at 863. Here we refer to Absolute and Magnus collectively as "Absolute" because all claims against them apply to both.

187 *Id.*

188 *Id.*

189 *Id.*

190 *Id.* at 864-865.

191 *Id.* at 865. (internal quotes omitted) (citing *United States v. King*, 227 F.3d 732, 743-44 (6th Cir. 2000)).

192 *Id.*

193 *Id.* at 865-867.

194 *Id.* at 867-868.

195 *Id.* at 868-869.

196 *Id.* (citations omitted).

197 *Id.* at 874-875.

198 *Id.* at 875.

199 *Id.* at 875-876.

200 *Id.* at 876-877.

201 *Id.* at 877-878.

202 *Id.* at 871.

203 *Id.* at 871-872.

204 *Id.* at 872. Absolute also raised the good-faith defense set forth in 18 U.S.C. § 2520(d), which provides a "complete defense" against any civil or criminal action where a person acted in good-faith reliance on provisions permitting certain actions by electronic communication service providers and people acting under color of law. The court rejected this argument because Absolute was neither providing an electronic communications service nor acting under color of law.

205 *Id.* at 872-874.

206 *Id.* at 879-881.
207 *Id.* at 879. (citing *Housh v. Peth*, 133 N.E.2d 340 (Ohio 1956)).
208 *Id.* at 879-881.
209 *Id.* at 880-881.
210 *Id.* (citing *Quigley v. Rosenthal*, 327 F.3d 1044 (10th Cir. 2003)).
211 *Id.* at 881.
212 *Id*.
213 Andrew Welsh-Huggins, "Susan Clements-Jeffrey Settles Suit with Absolute Software Over Laptop Sex Images," *The Huffington Post*, September 7, 2011, http://www.huffingtonpost.com/2011/09/07/susan-clements-jeffrey-absolute-software_n_951943.html.
214 "Absolute Investigations / Team," Absolute Software, http://www.absolute.com/en/services/investigations/team.
215 *Id.*
216 Deposition of Kyle Magnus, *Clements-Jeffrey v. City of Springfield*, No. 3:09-cv-00084-WHR (S.D. Ohio Oct. 22, 2010), ECF No. 77-1, p. 3.
217 "Absolute Investigations / Our Process," Absolute Software, http://www.absolute.com/en/services/investigations/process.
218 Larry Magid, "Many Ways to Activate Webcams Sans Spy Software," *CNET*, February 22, 2010, http://www.cnet.com/news/many-ways-to-activate-webcams-sans-spy-software/.
219 *Clements-Jeffrey v. City of Springfield*, 810 F.Supp.2d 857, 868-69 (S.D. Ohio 2011) (citations omitted).
220 *Clements-Jeffrey v. City of Springfield*, 810 F.Supp.2d 857, 869 (S.D. Ohio 2011); Deposition of Kyle Magnus, *Clements-Jeffrey v. City of Springfield*, No. 3:09-cv-00084-WHR (S.D. Ohio Oct. 22, 2010), ECF No. 77-1, p. 23; Deposition of Geoffrey R. Ashworth, *Clements-Jeffrey v. City of Springfield*, No. 3:09-cv-00084-WHR (S.D. Ohio Sept. 20, 2010), ECF No. 67-1, pp. 13-14.
221 Deposition of Susan Clements-Jeffrey (Vol. 1), *Clements-Jeffrey v. City of Springfield*, No. 3:09-cv-00084-WHR (S.D. Ohio Sept. 20, 2010), ECF No. 65-1, p. 38.
222 *U.S. v. Jacobsen*, 466 U.S. 109, 113 (1984).
223 Hidden, http://hiddenapp.com/.
224 Brandon Griggs, "'This Guy Has My MacBook!' Blog, Tweets Help Recover Stolen Computer," *CNN*, June 3, 2011, http://edition.cnn.com/2011/TECH/web/06/02/stolen.laptop.returned/; "This Guy Has My MacBook," http://thisguyhasmymacbook.tumblr.com/.
225 http://www.gotomypc.com/remote-access/.
226 Larry Magid, "Many Ways to Activate Webcams Sans Spy Software," *CNET*, February 22, 2010, http://www.cnet.com/news/many-ways-to-activate-webcams-sans-spy-software/.
227 Nate Anderson, "Meet the Men Who Spy on Women Through Their Webcams," *Ars Technica*, March 10, 2013, http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/.
228 Ian Parker, "The Story of a Suicide," *The New Yorker*, February 6, 2012, http://www.newyorker.com/reporting/2012/02/06/120206fa_fact_parker.
229 *Id.*
230 *Id.*
231 *Id.*
232 *See* Lori Andrews, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* 116 (New York: Free Press 2011).

233 Megan DeMarco, "Live Coverage: Dharun Ravi Found Guilty on Most Counts in Webcam Spying Trial Verdict," *NJ.com*, March 16, 2012, http://www.nj.com/news/index.ssf/2012/03/ravi_webcam_trial_verdict.html; Ian Parker, "The Story of a Suicide," *The New Yorker*, February 6, 2012, http://www.newyorker.com/reporting/2012/02/06/120206fa_fact_parker.

234 Becky Bratu, "Former Rutgers Student Dharun Ravi Sentenced to 30-Day Jail Term in Webcam Spying Case," *NBC News*, May 21, 2012, http://usnews.nbcnews.com/_news/2012/05/21/11791131-former-rutgers-student-dharun-ravi-sentenced-to-30-day-jail-term-in-webcam-spying-case.

235 The acronym RAT in this context can stand for either Remote Administration Tool or Remote Access Trojan. The two terms appear to be used interchangeably. *See, e.g.*, Mary Landesman, "Remote Access Trojan," *About.com*, http://antivirus.about.com/od/whatisavirus/g/rat.htm; Margaret Rouse, "What is a RAT (Remote Access Trojan)?" *TechTarget*, http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan (last updated October 2009). "Remote Access Trojan" is used here because the term more clearly connotes the user's intent to gain unauthorized access to a computer.

236 Nate Anderson, "Meet the Men Who Spy on Women Through Their Webcams," *Ars Technica*, March 10, 2013, http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/.

237 *Id.*

238 *Id.*

239 Charles Wilson, "Feds: Online 'Sextortion' of Teens on the Rise," *NBC News*, August 15, 2010, http://www.nbcnews.com/id/38714259/ns/technology_and_science-security/t/feds-online-sextortion-teens-rise; Nate Anderson, "How an Omniscient Internet 'Sextortionist' Ruined the Lives of Teen Girls," *Ars Technica*, September 7, 2011, http://arstechnica.com/tech-policy/2011/09/how-an-omniscient-internet-sextortionist-ruined-lives/.

240 Nate Anderson, "How an Omniscient Internet 'Sextortionist' Ruined the Lives of Teen Girls," *Ars Technica*, September 7, 2011, http://arstechnica.com/tech-policy/2011/09/how-an-omniscient-internet-sextortionist-ruined-lives/.

241 *Id.*

242 Judgment and Probation/Commitment Order, *U.S. v. Mijangos*, No. 2:10-cr-00743-GHK (C. D. Cal. Sept. 8, 2011), ECF No. 76.

243 Nate Anderson, "Webcam Spying Goes Mainstream as Miss Teen USA Describes Hack," *Ars Technica*, August 16, 2013, http://arstechnica.com/tech-policy/2013/08/webcam-spying-goes-mainstream-as-miss-teen-usa-describes-hack/.

244 *Id.*

245 Complaint, *U.S. v. Abrahams*, No. 8:13-mj-00422 (C. D. Cal. Sept. 17, 2013), ECF No. 1, p. 8.

246 Nate Anderson, "How the FBI Found Miss Teen USA's Webcam Spy," *Ars Technica*, September 27, 2013, http://arstechnica.com/tech-policy/2013/09/miss-teen-usas-webcam-spy-called-himself-cutefuzzypuppy/; Complaint, *U.S. v. Abrahams*, No. 8:13-mj-00422 (C. D. Cal. Sept. 17, 2013), ECF No. 1.

247 Nate Anderson, "How the FBI Found Miss Teen USA's Webcam Spy," *Ars Technica*, September 27, 2013, http://arstechnica.com/tech-policy/2013/09/miss-teen-usas-webcam-spy-called-himself-cutefuzzypuppy/.

248 Carol Kuruvilla, "New Miss Teen USA Claims She was the Victim of an Online Extortion Plot," *New York Daily News*, August 13, 2013, http://www.nydailynews.com/news/national/new-teen-

usa-claims-victim-online-extortion-plot-article-1.1426065.

249 Cyrus Farivar, "Sextortionist Who Hacked Miss Teen USA's Computer Sentenced to 18 Months," *Ars Technica*, March 17, 2014, http://arstechnica.com/tech-policy/2014/03/sextortionist-who-hacked-miss-teen-usas-computer-sentenced-to-18-months/.

250 Julianne Pepitone, "'Creepware' Hacker Sting Nets 97 Worldwide," *NBC News*, May 19, 2014, http://www.nbcnews.com/tech/security/creepware-hacker-sting-nets-97-worldwide-n109061; Brian Krebs, "'Blackshades' Trojan Users Had It Coming," *Krebs on Security*, May 19, 2014, http://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/.

251 Brian Krebs, "'Blackshades' Trojan Users Had It Coming," *Krebs on Security*, May 19, 2014, http://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/.

252 Julianne Pepitone, "'Creepware' Hacker Sting Nets 97 Worldwide," *NBC News*, May 19, 2014, http://www.nbcnews.com/tech/security/creepware-hacker-sting-nets-97-worldwide-n109061.

253 Brian Krebs, "'Blackshades' Trojan Users Had It Coming," *Krebs on Security*, May 19, 2014, http://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/.

254 Julianne Pepitone, "'Creepware' Hacker Sting Nets 97 Worldwide," *NBC News*, May 19, 2014, http://www.nbcnews.com/tech/security/creepware-hacker-sting-nets-97-worldwide-n109061.

255 *Id.*

256 Alex Hern, "FBI Arrests 100 Hackers over Blackshades Malware," *The Guardian*, May 19, 2014, http://www.theguardian.com/technology/2014/may/19/fbi-arrests-100-hackers-blackshades-rat-backdoor-malware.

257 National Crime Agency, "Multiple UK Arrests in International Operation to Combat Computer Hijackers," November 21, 2014, http://www.nationalcrimeagency.gov.uk/news/news-listings/491-multiple-uk-arrests-in-international-operation-to-combat-computer-hijackers.

258 *See, e.g.*, Ala. Code 1975 § 13A-8-112(a)(4); Ariz. Rev. Stat. Ann. § 13-2316(A)(3); Ark. Code. Ann. § 5-41-202(a)(5); Cal. Penal Code Ann. § 502(c)(8); Colo. Rev. Stat. Ann. § 18-5.5-102(1)(f); Fla. Stat. Ann. § 815.06(2)(e); Ga. Code Ann. § 16-9-152; La. Stat. Ann. §14:73.7(A)(4); 17-A Me. Rev. Stat. § 432(1); Mich. Comp. Laws Ann. § 752.795(b); Miss. Code. Ann. § 97-45-3(1)(c); N.H. Rev. Stat. Ann. § 638:17(VI); N.D. Cent. Code Ann. § 12.1-06.1-08(2); Ohio Rev. Code Ann. § 2909.07(A)(6)(b); S.C. Code § 16-16-20(1)(b); Tenn. Code §§ 39-14-602(b)(3); W. Va. Code §§ 61-3c-7.

259 Spencer Ackerman, "Senators to Investigate NSA Role in GCHQ 'Optic Nerve' Webcam Spying," *The Guardian*, February 28, 2014, http://www.theguardian.com/world/2014/feb/28/nsa-gchq-webcam-spy-program-senate-investigation.

260 Electronic Frontier Foundation, "EFF Demands Release of More Secret Surveillance Court Rulings," EFF Press Release, (May 1, 2014), https://www.eff.org/press/releases/eff-demands-release-more-secret-surveillance-rulings-fisa-court; Robyn Greene, "When is Enough Enough? Government Surveillance Skyrockets in 2010," ACLU, (May 9, 2011), https://www.aclu.org/blog/national-security/when-enough-enough-government-surveillance-skyrockets-2010-0.

261 N.J.S. 18A: 36-39; *see also* Martin Bricketto, "Christie Signs Student Privacy Bill in Wake of Laptop Scandal," *Law360*, April 15, 2013, http://www.law360.com/articles/432816/christie-

signs-student-privacy-bill-in-wake-of-laptop-scandal.

262 N.J.S. 18A: 36-39; *see also* Martin Bricketto, "Christie Signs Student Privacy Bill in Wake of Laptop Scandal," *Law360*, April 15, 2013, http://www.law360.com/articles/432816/christie-signs-student-privacy-bill-in-wake-of-laptop-scandal.

263 N.J.S. 18A: 36-39; *see also* Martin Bricketto, "Christie Signs Student Privacy Bill in Wake of Laptop Scandal," *Law360*, April 15, 2013, http://www.law360.com/articles/432816/christie-signs-student-privacy-bill-in-wake-of-laptop-scandal.

264 Kevin Bankston, Electronic Frontier Foundation, "Senators Introduce Bill in Response to EFF's Call for New Protections Against Secret Video Surveillance," April 15, 2010, https://www.eff.org/deeplinks/2010/04/senators-introduce-bill-response-effs-call-new; *see also* https://www.govtrack.us/congress/bills/111/s3214.

265 *United States v. Kyllo*, 553 U.S. 27 (2001); Jonathan L. Hafetz, "'A Man's Home is His Castle?': Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries," 8 *Wm. & Mary Journal of Women and the Law* 175 (2002).

266 U.S. Const. Am. III; *see also Griswold v. Connecticut*, 381 U.S. 479, 484 (1965) (citing the Third Amendment in support of the existence of a constitutional right to privacy).

267 *U.S. v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (holding that the U.S. District Court for the District of New Jersey was an improper venue for the criminal prosecution of an Arkansas resident who allegedly hacked computer servers located in Dallas, Texas and Atlanta, Georgia).

268 The user of a rented computer should be considered "another person" with respect to the rental company or another computer owner.

IMAGE CREDITS

"Globe centered in the Atlantic Ocean (green and grey globe scheme)" by Luan, used under CC BY-SA 3.0 | saturated from original (http://commons.wikimedia.org/wiki/File:Globe_centered_in_the_Atlantic_Ocean_%28green_and_grey_globe_scheme%29.svg)

"Washington city silhouettes on July 4th" by Vector Open Stock, used under CC BY 4.0 | saturated and cropped from original (https://www.vectoropenstock.com/vectors/preview/70796/washington-city-silhouettes-on-july-4th)