DECEMBER CLE BY THE HOUR

Sponsored By:

The Shreveport Bar Association

TECHNOLOGY IN THE COURTS: 2019 UPDATE

Melissa Allen

United States Fifth Circuit Court of Appeals

Technology in the Courts: 2019 Update

December CLE by the Hour Seminar December 11, 2019

Presented by:
Melissa Allen, United States Fifth Circuit Court of Appeals

I. Technology Laws[1]

A. Federal Communications Act of 1934 (47 U.S.C. § 151, et seq.)

Provides that no person "not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person." 47 U.S.C.A. § 605.

> *Nardone v. United States*, 308 U.S. 338 (1939) - Held that § 605 prohibits divulging such communications in federal criminal prosecutions and prohibits the use of information thus obtained in such prosecutions (the "fruits of the poisonous tree" doctrine). *See also Lee v. State of Fla*., 392 U.S. 378 (1968).

The mere interception of a telephone communication by an unauthorized person does not in and of itself constitute a violation of § 605. Only where the interception is followed by the divulging of the communication, as by introducing it into evidence, would there be a violation of § 605.

1 *See* mwl-law.com.

B. Federal Wiretap Act (18 U.S.C. § 2520)

Protects individual privacy in communications with other people by imposing civil and criminal liability for intentionally intercepting communications using a device, unless that interception falls within one of the exceptions in the statute.

Although the Federal Wiretap Act originally covered only wire and oral conversations (e.g., using a device to listen in on telephone conversations), it was amended in 1986 to cover electronic communications as well (e.g., emails or other messages sent via the Internet).

C. Electronic Communications Privacy Act (ECPA) of 1986 (18 U.S.C. § 2510, et seq.)

Prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Allows employers to listen to "job-related" conversations. Protects the privacy of wire, oral, and electronic communications including telephone conversations (18 U.S.C. §§ 2510 to 2522). Gives employers almost total freedom to listen to any phone conversation, since it can be argued that it takes a few minutes to decide if a call is personal or job-related. This exception applies only to the employer, not the employee. Permits telephone call recording if at least one party consents. Call recording is unlawful if the party consents with the intent to use the recording to commit a criminal or tortious act.

Exceptions to the Federal Wiretap Act's one-party consent requirement include call recordings captured by:

- Law enforcement;
- Communication service providers, if the recording is necessary to deliver service, or protect property or rights;
- Federal Communications Commission (FCC) personnel for enforcement purposes;
- Surveillance activities under the Foreign Intelligence Surveillance Act (50 U.S.C. §§ 1801 to 1813);

• Individuals, if they record telephone calls to identify the source of harmful radio or other electronic interference with lawful telephone calls or electronic equipment;
• Court order.

D. Stored Communications Act (18 U.S.C. § 2701, et seq.)

Part of the Electronic Communications Privacy Act. Creates privacy protections for the content of stored communications and the related non-content information. Ex. Emails, cell phone records.

E. Electronic Eavesdropping

To overhear, record, amplify, or transmit any part of the private communication of others without the consent of at least one of the persons engaged in the communication. It may involve the placement of a "bug" inside private premises to secretly record conversations, or the use of a "wired" government informant to record conversations that occur within the informant's earshot.

F. Wiretapping

Wiretapping is a form of electronic eavesdropping accomplished by seizing or overhearing communications by means of a concealed recording or listening device connected to the transmission line. Where a message is overheard by a third person during its transmission and there has been no disturbance of the physical integrity of the communication system, it is less clear that an illegal "interception" has taken place.

Olmstead v. United States, 277 U.S. 43 (1928) held that the Fourth Amendment's search and seizure commands did not apply to government wiretapping accomplished without a trespass onto private property.

Superseded by *Katz v. US*, 389 U.S. 347 (1967), which established a citizen's right to privacy and requires law

enforcement to obtain a warrant before wiretapping a phone conversation.

US v. Carpenter, 138 S. Ct. 2206 (2018) held that the government's acquisition of person's cell-site records from their wireless carrier was a Fourth Amendment search and therefore the government must obtain a warrant supported by probable cause before acquiring the records.

G. Intercepted communication

The aural (or heard) acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

H. State Laws on Recording Conversations

Individuals, businesses, and the government often have a need to record telephone conversations that relate to their business, customers, or business dealings. The U.S. Congress and most states' legislatures have passed telephone call recording statutes and regulations that may require the person wanting to record the conversation to provide notice and obtain consent before doing so.

Most states require one-party consent, which can come from the person recording if present on the call. Some states require that all parties to a call consent to recording. Laws governing telephone call recording are typically found within state criminal statutes and codes because most states frame call recording as eavesdropping, wiretapping, or as a type of intercepted communication. State laws may not explicitly mention telephone call recording because of these technical definitions.

Counsel may need to infer when and under what circumstances a state permits telephone call recording by reviewing prohibited actions. The big issue when it comes to recording someone is whether the jurisdiction you are in requires that you get the consent of the person or persons being recorded.

Interstate communications: Telephone calls are routinely originated in one state

and participated in by residents of another state. In conference call settings, multiple states (and even countries) could be participating in a telephone call which is subject to being recorded by one or more parties to the call. Some states require the consent of all parties to the conversation. Others require only the consent of one party. It is not always clear whether federal or state law applies, and if state law applies which of the two (or more) relevant state laws controls.

Usually, the law of the jurisdiction in which the recording device is located will apply.

Some jurisdictions, however, take a different approach when addressing this issue and apply the law of the state in which the person being recorded is located.

When recording a call with parties in multiple states, it is best to comply with the strictest laws that may apply or get the consent of all parties. It is generally legal to record a conversation where all the parties to it consent.

1. Consent

In some states, "consent" is given if the parties to the call are clearly notified that the conversation will be recorded, and they engage in the conversation anyway. Ex. A customer service department recorded voice warning, "This call may be recorded for quality assurance or training purposes."

It is usually a good practice for practitioners to let the witness know they are recording the conversation to accurately recall and commemorate the testimony being given – such as during the taking of a witness' statement.

a. One-Party Consent

If the consent of one party is required, you can record a conversation if you are a party to the conversation. If you are not a party to the conversation, you can record a conversation or phone call provided one party consents to it after having full knowledge and notice that the conversation will be recorded.

18 U.S.C. § 2511(2)(d) requires only that one party give consent.

Thirty-eight states (including Texas & Louisiana) and the District of Columbia have adopted a "one-party" consent requirement.

b. All-Party Consent

Eleven (11) states require the consent of everybody involved in a conversation or phone call before the conversation can be recorded. Those states are: California, Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania and Washington.

Referred to as "two-party" consent laws but, technically, require that all parties to a conversation must give consent before the conversation can be recorded.

2. Louisiana (La. Rev. Stat. Ann. § 15:1303(c)(4))

One-Party Consent State. The Electric Surveillance Act bars the interception, recording or disclosure of and oral or telephonic communication by the means of an electronic recording device without the consent of at least one party or if they are a party to said communication.

3. Texas (Tex. Penal Code Ann. § 16.02; Tex. Code Crim. Proc. Ann. art. 18.20)

One-Party Consent State. It is not unlawful for an individual who is a party to or has consent from a party of an in-person or electronic communication to record and or disclose the content of said communication unless the person is doing so for the purpose of committing a tortious or criminal act. An individual may also disclose the content of any electronic communication that is readily accessible

to the general public.

I. Exceptions

Common exceptions found in a majority of states' laws include recordings captured by police, court order, communication service providers, emergency services, etc. Generally, it is permissible to record conversations if all parties to the conversation are aware and consent to the interception of the communication. There are certain limited exceptions to the general prohibition against electronic surveillance. For example, "providers of wire or electronic communication service" (e.g., telephone companies) and law enforcement in the furtherance of criminal investigative activities have certain abilities to eavesdrop.

J. Video Recordings[2]

Most video recordings are legal with or without consent. Very few laws prohibit video recording of any kind, but there are some laws prohibiting video recordings in areas of expected privacy without consent.

Hidden video cameras are legal to sell, purchase, own, and possess.

The usage of hidden video cameras is legal in most cases, however, the use may be illegal if the hidden cameras are used in prohibited areas.

Ex. Bathrooms, locker rooms, changing/dressing rooms, adult bedrooms, and other areas where a person should expect a high level of personal privacy.

Most laws dealing with video recording privacy issues allow surreptitious recording and monitoring of video activity under most circumstances without notification of any of the parties involved as long as there is no reasonable expectation of privacy. In public, there is usually no reasonable expectation of privacy.

2 *See* theverge.com & palmvid.com

* You can record others in your home unless it is somewhere they would have a reasonable expectation of privacy like the bathroom.

*In some cases, courts have allowed video recordings of nannies, elder care employees, and other types of video recordings made with covert cameras without the subject's consent.

* Other people cannot record you in your home without your permission.
* You cannot record inside private businesses or governmental entities if they prohibit it. Otherwise you can.

1. Snapchat, Instagram, Twitter & Vine

* United States laws provide a lot of protection to websites.
* The poster is the person who would have any legal ramifications, not the website.

* Our laws require that if the post violates the law, whether it's violating copyright or violating child pornography rules or some other law, there must be a methodology through which one can ask the website to take it down.

* The recorder of the video owns the video and has the choice whether to enforce the copyright to it.

* If someone records a video of someone else in public, they can post it without legal ramifications unless they profit from it. If they profit, they may be forced to give up the money if they are sued by the person who is the subject of the video.

2. Police Recordings

* The public in general has the right to record the police in public places.

* Caveat – You cannot record them if it interferes with their ability to do their job. You must give them space while you are recording.

* Police can also record others without their consent. Ex. Body cams.

* Although you have a reasonable expectation of privacy in your home this disappears when the police enter, esp. with a warrant. However, the admission into evidence of the recording itself may be disputed later.

NOTE: Recording audio is very different from video. There are specific federal and state laws prohibiting surreptitious recording and monitoring of audio conversations. These laws are taken very seriously by authorities and failure to abide by them may result in severe consequences.

II. Who is Spying on You?[3]

A. Smart Phones, Tablets, Laptops, Webcams & Apps

Anything with a voice assistant or microphone can potentially record you – whether turned on or off.

Anything with a camera can potentially surveille you – whether turned on or off.

Smart Phones & Tablets

Your voice triggers smart speakers and smartphones.

Your smartphone/tablet is similar to smart speakers like the Amazon Echo and Google Home -- they listen for "wake" words like "Hey Siri" and "Okay Google" all the time. These wake words are required for your smartphone to actually start recording.

In some cases, third-party apps like Facebook or Instagram have access to this local data and use it for advertising.

Using voice tracking for marketing purposes is legal because the privacy policies and end-user agreements you agreed with plus current laws allow it.

Ma v. Apple Inc., 5:14-cv-003344 (USDC NDCA 7/24/14) - In 2014, a class action suit was filed against Apple alleging that users were being spied on and

3 *See* mindchasers.com; www.komando.com; http//:pando.com; www.macrumors.com; www.popularmechnics.com; www.bbc.com; www.digitalspy.com; http://ios.gadgethacks.com; www.consumerreports.org; www.forbes.com; www.lifewire.com; www.mccall.com.

tracked with the phone's location tracking tools. Plaintiff in this case alleged that while using her iPhone, her daily whereabouts were tracked, recorded, and transmitted to an Apple database where they were stored for future reference.

Williams v. Apple Inc.; Doe Defendants (Houston, 2019) - Houston attorney Larry D. Williams II filed a lawsuit against Apple in January of 2019 claiming the bug allowed for someone to eavesdrop on a private deposition he had with a client. According to the lawsuit, Williams did not misuse the iPhone in any way, and yet the FaceTime bug "allowed for the recording of a private deposition."

> By exploiting a bug in Group FaceTime, a person could force a FaceTime connection with another person, providing access to a user's audio and sometimes video even when the FaceTime call was not accepted.

Williams claims that Apple has "failed to provide sufficient warnings and instructions that would have put Plaintiff and the general public on notice of the dangers and adverse effects caused by the update to iOS 12.1." Williams seeks punitive damages against Apple and unknown parties, claiming "product liability, negligence, warranty and fraudulent misrepresentation."

Apple revealed it was aware of the issue on Jan. 28, and the company disabled group FaceTime later that day, neutralizing the bug. A software update was subsequently released addressing the issue.

<u>Prevention & Protection</u>

* *Disable "Hey Siri"* - With iOS 8, Apple introduced the "Hey Siri" wake phrase, so you can summon Siri without even touching your iPhone. If you turn this feature on, this means your iPhone's mic is always listening, waiting for the phrase "Hey Siri."

Apple says this is processed locally on the device and your iOS device does not start recording your voice until it hears "Hey Siri." Once your request is recorded, it then uploads the audio file to Apple's servers for processing.

To turn off "Hey Siri:" Navigate to your iOS device's Settings >> General

>> Siri, then toggle Allow "Hey Siri" to off.

* *Disable "Ok Google"* - Google recently released “OK Google.” This serves as Google’s new wake phrase, just like “Alexa” and “Hey Siri,” calling the attention of Google Assistant on Google Home speakers, Android smartphones, and the Chrome browser. Every time you use "OK Google" or use another voice-controlled function, your request is recorded and the snippets are saved to your Google account. Google now features a My Account tool that lets you access your recordings and delete them if you want. You can also tell Google to stop recording your voice for good.

To turn off the "OK Google" wake phrase: On Android, just go to Settings >> Google >> Search & Now >> Voice and turn “OK Google” detection off.

* *Disable "Hey Cortana"* – Cortana is the voice-activated system from Microsoft. Similar to the others on this list, Cortana can answer questions, do searches, set appointments, and open applications. The wake phrase is "Hey Cortana."

To turn off "Hey Cortana:" Open Cortana on your Windows computer, select the Notebook icon in the right column, click on Settings then toggle "Hey Cortana" to off.

* *Disable Facebook's mic access* - If you are an iPhone user, go to Settings >> Facebook >> Settings >> slide the Microphone switch to the left so it turns from green to white. That turns it off.

Alternatively, go to Settings >> Privacy >> Microphone >> look for Facebook then do the same. Note that you can toggle the mic on and off for other apps, too.

For Android users: Try Settings >> Applications >> Application Manager >> look for Facebook >> Permissions >> Turn off the mic.

Laptops & Webcams

* Victims of webcam hacks have seen images and videos of themselves – in

compromising situations – uploaded to voyerism websites.

* There are several ways hackers have gained access to people's webcams but the most common is through the use of Trojan horse malware. This is malicious code hidden within seemingly innocent files that once downloaded will do its thing and give the hackers backdoor control of your device.

Prevention & Protection: Anti-virus software and a physical cover over the camera.

Apps

Over 250 apps available across the Apple App Store and the Google Play Store are programmed to be able to listen for audio through a phone's microphone. Using code from a company called Alphonso, the apps would listen for audio from television shows or ads to more precisely target advertisements after displaying a warning message.

Using a smartphone's microphone, Alphonso's software can detail what people watch by identifying audio signals in TV ads and shows, sometimes even matching that information with the places people visit and the movies they see. The information can then be used to target ads more precisely and to try to analyze things like which ads prompted a person to go to a car dealership.

* Tinder (dating app) – Has tested an update that would share a user's exact location with other users

* WhatsApp – A flaw was identified in the app which would allow an intruder to plant spyware on a phone with one missed call. Once the spyware was installed, the phone's microphone could be turned on and encrypted chats, photos, and other information could be taken out of the phone.

* Gaming Apps - Certain mobile gaming apps track their users by listening to certain sounds through their smartphone's mic. Using software from Alphonso, which collects viewing data for advertisers, certain gaming applications can use your phone's microphone to learn what you watch, listening in the background for audio signals playing from your TV, including gaming consoles, TV shows,

streaming programs, and advertisements. The information is then analyzed and paired with your location to learn for example which ads resulted in you going to a restaurant or retailer.

Prevention & Protection:

Do not give Microphone access to apps.

Remove Microphone access to third-party apps.

Disable Location Services in the Privacy tab on your iPhone and tablet.

Spyware Apps

1. **TheOneSpy** - App that specifically targets gadgets that run on iOS. Once the software is installed, whoever installed it is in possession of everything that happens on that particular device. All of the data collected by TheOneSpy is encrypted and sent to a web portal where a spy can review it. This means someone could be reading your sent and received text messages and emails, listening to recordings of your phone calls, snooping through your browsing history and more. TheOneSpy can also activate the microphone and camera on your device to spy on your surroundings.

2. **Highster Mobile** - Monitor other apps you use on your device, such as Facebook, Instagram, Skype, WhatsApp, etc. It can be installed remotely, and can block any app it's told to. Has the ability to access messages and data that have been deleted. Can also be used to completely lock a targeted phone, which means you could lose access to your device entirely.

3. **FlexiSpy** - Can be installed on your device to spy on activity. Monitors messages, audio and data, it can spy on your GPS location, passwords, and other apps. Whoever installed the app can receive alerts for various triggers, and can spy on you in secret since the application is hidden from the task manager.

4. **mSpy** - Monitors content from apps like SnapChat. It can also monitor your GPS location, and restrict incoming calls from a predefined number. Marketed toward parents who are worried about their child being contacted by someone they don't trust.

5. **Spyera** - An entire smartphone. The app comes pre-installed on various Apple and Android devices, so whoever gives you the phone can monitor all of your personal activity. Software can listen in on phone calls and can use your microphone to listen in on everything else that's happening near the smartphone. Can also track your instant messages and texts, upload copies of the photos you take, spy on conversations held through other apps like Skype, Viber, WeChat, etc., log everything you type, and use the camera to spy on you physically.

Prevention & Protection

You can purchase antispyware software which detects and removes spyware.

Signs spyware may be on your phone:

Abnormally high data usage
Cell phone shows signs of activity in standby mode
Unexpected reboot
Odd sounds during calls
Unexpected text messages
Deteriorating battery life
Increasing battery temp in idle mode
Increased shut down duration
Difficulty shutting down your device
Cell phone grows increasingly slower

B. Smart TVs

Smart TVs are sets that connect to the internet, making it easy stream videos from services such as Netflix.

Smart TVs collect data about what you watch with a technology called automatic content recognition (ACR). ACR attempts to identify every show you play on the TV—including cable, over-the-air broadcasts, streaming services, and DVDs and Blu-ray discs—and sends the data to the TV maker or one of its business partners, or both. ACR helps the TV recommend other shows you might want to watch. It is also used for targeting ads to you and your family, and for other marketing purposes.

Prevention & Protection:

You can deny permission for ACR as you set up the TV—do not just click "okay" to all the privacy policies and user agreements.

For instructions on how to disable ACR on specific brands of smart tvs, go to https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features/

C. Home & Other Security Cameras

If you install smart security cameras in your home or office you need to be aware of certain legal issues so that you do not violate statutory restrictions or infringe on anyone's privacy. The critical legal issue is the consent of all parties to be monitored or recorded, and whether there is a reasonable expectation of privacy. Meaning, whether it would be understood or logically inferred that one is being watched, listened to, or recorded.

Ring – Camera-equipped doorbell. Amazon purchased Ring for $1 billion in February of 2018. A security flaw was discovered in the software that allowed people who were logged into the doorbell app to stay logged in even after the password had been changed, viewing anything that the camera viewed.

Nest Cam - The devices can be configured to watch and listen remotely with remarkably high definition quality. All indications of monitoring (red light and chime) can be disabled so that the camera appears inactive. In audio monitor mode, the gain or sensitivity of the microphone can be increased from 0-100%. Sound within a room can trigger an alert within their application. The subscription recording application allows the review of video and audio that has been captured during the past ten or thirty-day period. It allows the targeting of a specific date and time, and compressed playback to create a time lapse sequence. The system works just like a DVR and allows rewind and fast forward functions for searching of content.

NOTE: Any video and audio that may be stored in the Cloud can be subject to a search warrant by law enforcement.

D. Baby Monitors

Baby monitors have repeatedly been the subjects of unlawful viewing.

Voyeurs - Hackers that want to peer into parents and their children's lives and listen to their private conversations.

Pranksters - Some internet-connected baby monitors feature the ability for parents to talk back to the baby via a speaker on the baby monitor's camera. The idea was that you could tell the baby "go back to sleep" or something and calm them down without having to go in their room and further disturb them. Pranksters will purposely hack into baby monitors to use the talkback feature to try and scare the baby and/or the parents.

Criminals - Users steal personal information that was heard over the microphone for fraud, theft, blackmail, extortion, etc.

Prevention & Protection:

Check the manufacturer's website for updated firmware (the software built into the camera's hardware that runs everything) that fixes a security issue or some other software flaw.

Create a strong password for the camera log in.

Set It to Local Network Only. Restricting the connection to the local network only may greatly reduce the chance of your monitor being hacked.

Secure your home network and wireless router.

E. Vehicles

Car that connect to the Internet can collect vast amounts of data about drivers, such as where you went to dinner, if you broke the speed limit or if your seat belt was buckled.

When you buy a car, you cede data control to your car company. Most automakers say they will not sell information without an owner's consent but they are not legally required to inform you if they do.

Under federal law, drivers own data stored in event data recorders, or "black boxes," which monitor vehicles in a crash. Police and insurers need a driver's consent — or a court order — to get that data. But there are no laws addressing data collected by automakers through vehicle internet connections.

1. Onstar & Sirius XM

(1) In 2014 a warrant was issued that allowed New York police to trace a vehicle by demanding the satellite radio and telematics provider SiriusXM provide location information. The warrant, originally filed in 2014 but only recently unsealed, asked SiriusXM "to activate and monitor as a tracking device the SIRIUS XM Satellite Radio installed on the Target Vehicle for a period of 10 days." The target was a Toyota 4-Runner wrapped up in an alleged illegal gambling enterprise.

SiriusXM complied with the order and by switching on the stolen vehicle recovery feature of its Connected Vehicle Services technology. Sirius says it also works sporadically with law enforcement to provide such information, always requiring a valid warrant. It estimates it receives five valid court orders a year to activate the stolen vehicle recovery feature to monitor a suspect.

(2) In December 2009 police asked GM to turn over OnStar data from a Chevrolet Tahoe rented by a suspected crack cocaine dealer Riley Dantzler. The cops who were after Dantzler had no idea what the car looked like or where it was, but with OnStar tracking they could follow him from Houston, Texas, to Ouchita Parish, Louisiana. OnStar's tracking was able to "identify that vehicle among the many that were on Interstate 20 that evening." They stopped Dantzler and found cocaine, ecstasy and a gun inside.

(3) In 2007, suspected heroin dealer Lamauro Coleman was tracked after OnStar was ordered to continuously reveal the physical location of the defendant's GMC Envoy SUV as he travelled around Michigan. When he was stopped and searched, the cops found 43 grams of heroin.

(40 In 2007, the OnStar system in a Chevrolet Tahoe belonging to a Gareth Wilson in Ohio contacted OnStar staff when an emergency button was pushed. As noted in a 2008 opinion from the case, Wilson was unaware the button had been pushed. Subsequently, an OnStar employee heard the occupants discussing a possible drug deal, and allowed an officer from the Fairfield County Sheriff's Office to listen to the conversation. When the vehicle was located and searched, marijuana was found and an indictment filed days later. Ironically, the suspect had not even signed up to the OnStar service, but it had not been switched off.

2. Uber & Lyft

(1) Uber has been sued for using its software to track riders' whereabouts and transmit that information back to its executives. It settled the suit by agreeing to encrypt rider geo-location data.

(2) Lyft also uses insight software to view the personal contact information and ride history of its rider passengers.

F. Google, Gmail & Web Surfing

* Google saves years of information on purchases you have made, even outside Google, and pulls this information from Gmail.

* Gmail does scan all emails according to new Google terms.

* Google's system scans the content of emails stored on Google's servers as well as those being sent and received by any Google email account.

* Google has patented a Big Brother-style system that uses cameras and sensors to watch your kids and tell you when they have been misbehaving

The patent filed suggests smart homes of the future could monitor children with cameras, microphones, motion sensors and thermal imaging. The Google Home system could use this real-time information to decide if the person in question is misbehaving.

In another patent Google described a device that would give advice to

parents for “areas of improvement” such as spending more time with their children at supper.

* Google Nest is a brand of smart home products, including thermostats, smoke detectors, ceiling fans, lights and security systems including smart doorbells and smart locks. The products typically feature voice assistants and cameras.

* Some Google Nest mini home units have been secretly recording every sound they hear and transmitting all of that information back to Google. While it's unclear what happens to the recordings once they land at Google, the privacy implications are obvious.

G. Airbnb

Airbnb was sued in 2015 in federal court in California over a hidden camera in a rented apartment. The case concerns an Irvine, California apartment with a wireless camera allegedly installed in the living room. The plaintiff, a German woman named Yvonne Schumacher, stated she was unaware of the camera, which allegedly captured both naked footage and private conversations. The case alleged negligence against Airbnb itself, as well as charges of wiretapping, privacy intrusion, and infliction of emotional distress against the couple who rented the home.

Schumacher stayed in the apartment beginning on December 13, 2013 and was never informed of the camera. She slept and walked through the living room of the apartment without clothing believing that she was in an entirely private space.

> In 2017 an Airbnb user was arrested for video voyeurism after a couple noticed that he had installed a camera in the smoke detector that was pointed at the bed.

III. <u>Alexa & Amazon Echo</u>

A. The Class Action Lawsuits

(1) *C.O., a minor, et al v. Amazon.com, et al*, 2:19-cv-910 (USDC WDWA

6/11/19)

(2) *R.A., a minor, et al v. Amazon.com, Inc., et al*, Case No. 19STcv20205, California Superior Court, LA Central District (6/11/19)

The following are excerpts from the above two class action suits:

Millions of Americans use Amazon's smart-speaker technology ("Alexa") in their homes. People speak to Alexa-enabled devices such as the Echo or Echo Dot about everything from the mundane ("Alexa, what's the weather?") to the deeply personal ("Alexa, what are the symptoms of depression?").

Most people believe that when they speak to an Alexa-enabled device, it converts their voice into a set of digital computer instructions. They expect that this digital query is sent over the internet for processing, that a digital response is returned, and that the device then converts the response into Alexa's voice. They do not expect that Alexa is creating and storing a permanent recording of their voice.

This expectation is reasonable; it would be easy for Alexa to work this way, as numerous other voice-recognition technologies do. But Alexa does something else.

> *After Alexa processes a user's commands, Amazon saves a permanent recording of the user's voice to its own servers. It then analyzes and uses these voice recordings for its own commercial benefit. These uses include allowing workers around the world to listen to the voice recordings and creating voiceprints of users, which can be used to identify them when they speak to other devices in other locations. Amazon has thus built a massive database of billions of voice recordings containing the private details of millions of Americans.*

Amazon purports to obtain consent to record individuals who set up an Alexa-enabled device.

But there is a large group of individuals who do not consent to be recorded when using an Alexa-enabled device and who use Alexa without any understanding or warning that Amazon is recording and voiceprinting them: children. Alexa routinely records and voiceprints millions of children without their consent or the consent of their parents.

This practice violates the laws of Florida, Illinois, Michigan, Maryland, Massachusetts, New Hampshire, Pennsylvania, and Washington, which prohibit the recording of oral communications without the consent of all parties to the communication [state wiretap laws]. These laws recognize the unique privacy interest implicated by the recording of someone's voice. That privacy interest is all the more powerful in light of modern voiceprinting technology and the potentially invasive uses of big data by a company the size of Amazon. It takes no great leap of imagination to be concerned that Amazon is developing voiceprints for millions of children that could allow the company (and potentially governments) to track a child's use of Alexa-enabled devices in multiple locations and match those uses with a vast level of detail about the child's life, ranging from private questions they have asked Alexa to the products they have used in their home.

The prayers for relief includes:
Class action certification;
Declaring that Amazon's actions, as set out above, violate the state privacy laws cited herein;
Requiring Amazon to delete all recordings of the Class members, and to implement functionality to prevent further recording of the Class members without prior consent;
Awarding damages, including nominal, statutory, and punitive damages
Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees & interest;
Injunctive and declaratory relief

> The day after the suits were filed, Amazon announced the newest generation of its Echo Dot Kids speaker. Amazon clarified then that "none of the Alexa skills" in its "FreeTime" games and media service "have access to or collect personal information from children." Amazon added that "there are multiple ways to delete a child's profile or voice recordings."
>
> In May of this year, lawmakers and public interest groups called the Federal Trade Commission to investigate Amazon's Echo Dot Kids due to claims that the company was violating privacy rights by storing kids' recordings without parental consent.

IV. How Law Enforcement is Using Technology[4]

Communications Assistance for Law Enforcement Act (CALEA) (1994)

Requires providers of commercial voice services to engineer their networks in such a way as to assist law enforcement agencies in executing wiretap orders.

A. Social Media

The internet has become a broad web of shared personal information that remains permissible as evidence when attained legally, creating an organic database of recorded behaviors that can provide unique insight into each case. When analyzed, this data can even be useful in identifying criminal patterns and anticipating threats.

Everyday technologies like social media and other applications can be very helpful to law enforcement but they have also made it possible for gangs and terrorist organizations to coordinate like never before, creating an entirely new digital space that needs policing.

B. Crime Scene Imaging

3-D scanning technology takes a three-dimensional scan of an entire crime scene, replacing many sketches and photographs.

C. Radar Technology & Thermal Imaging

New through-the-wall radar technology uses radio waves to detect movement through walls. Thermal imaging technology senses heat and creates images based on heat patterns. Both implicate the Fourth Amendment.

* Both types of imaging could also be used for rescues.

4 *See* www.policemag.com; www.purdueglobal.edu; www.rasmussen.edu

Officers use both to assess a building or scene prior to entering to assess threat levels or for other law enforcement-related reasons.

D. Body Cams

There has been a recent national call for officers to wear cameras. These cameras, which are now small enough to be mounted on an officer's uniform or on a pair of glasses promote public trust and accountability in the age of viral videos and demands for transparency. Though some members of the law enforcement community have raised concerns over the use of the cameras, they can actually provide a helpful resource to police departments and protect officers from an increasing abundance of false claims of inappropriate behavior or abuse.

Every second of video that an officer's camera records can be taken into evidence, providing a first-hand account of what took place during any interaction with a subject. The cameras provide the officer's perspective on the incident unfettered by testimony and witness reports. Departments can also use the footage to train and practice crisis scenarios, reviewing successful arrests and discovering areas for improvement. Community members and law enforcement officers alike can benefit from police cameras seeing more frequent use.

E. Software, Data & Predictive Analytics

Using software dedicated to providing insight into criminal patterns and all legally warranted personal information, analysts are able to recognize connections between various activities and cases, even potentially predict where the next threat will emerge. These systems draw from a number of databases simultaneously, which helps law enforcement analyze information coming from mobile telephone service providers, banks, credit card companies, and many other public forms of data. Once all of the relevant information is gathered, new tools like these allow agencies to share their findings with others around the nation.

F. Rapid ID Systems

Rapid identification systems allow police officers to quickly see the criminal history of individuals through a basic search. People pulled over while driving without a license can still be identified instantly through an in-car computer search.

The FBI's Next Generation Identification (NGI) system uses biometrics—including fingerprints, palm prints, iris recognition, and facial recognition—to match up individuals with their criminal history information. Current technologies in the NGI are constantly being updated, and new ones are being added to make the NGI the most comprehensive way to glean up-to-date information on the person being examined.

G. Detection, Surveillance & GPS

GPS helps police officers get to crime scenes and locate criminals more easily. It also helps departments better manage police forces, since maps of police officer dissemination can ensure more areas are covered. The integration of GPS with other police systems helps make data more robust, as location services are seamlessly included in reporting.

H. Gunshot Technology

Gunshot technology detects gunfire and gives police officers instant access to shooting location maps, as well as information on how many shooters are present and how many shots were fired.

I. Drones & Robots

When police and military need an aerial view of a scene, drones can help law enforcement safely observe an area.

Robots are typically used for reconnaissance in dangerous situations and for bomb disposal. In the future, security robots that look for suspicious activity and patrol intersections may be introduced.

J. License Plate Scanning

Automatic license plate scanning technology enables police officers to instantly see if a car in their area has been stolen or if there is a warrant out for the arrest of the driver.

K. Tablets & Smartphones

iPads allow officers to do just about anything away from their department desk. Officers can now file accident and incident reports wirelessly, look up photos of suspects and access other information in a state crime database—all from their car or a crime scene.

V. The Dark Web v. The Deep Web[5]

A. Dark Web

The dark web is a part of the internet that isn't indexed by search engines.

You can buy credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts and software that helps you break into other people's computers. Buy login credentials to a $50,000 Bank of America account for $500. Get $3,000 in counterfeit $20 bills for $600. Buy seven prepaid debit cards, each with a $2,500 balance, for $500 (express shipping included). You can hire hackers to attack computers for you. You can buy usernames and passwords.

Accessing the dark web requires the use of an anonymizing browser called Tor. The Tor browser routes your web page requests through a series of proxy servers operated by thousands of volunteers around the globe, rendering your IP address unidentifiable and untraceable.

Dark web sites look like other sites, but there are important differences. One is the naming structure. Instead of ending in .com or .co, dark web sites end in .onion. Browsers with the appropriate proxy can reach these sites, but others cannot. Dark web sites also use a scrambled naming structure that creates URLs

5 *See* www.csoonline.com; www.cloudwards.net

that are often impossible to remember. For example, a popular commerce site called Dream Market goes by the unintelligible address of "eajwlvm3z2lcca76.onion."

The dark web uses bitcoin, the crypto-currency that enables two parties to conduct a trusted transaction without knowing each other's identity. Nearly all dark web commerce sites conduct transactions in bitcoin or some variant, but that does not mean it is safe to do business there. The inherent anonymity of the place attracts scammers and thieves.

If you find your own information on the dark web, there is not much you can do about it, but at least you will know that your information has been compromised.

B. Deep Web

Around 90 percent of online content is blocked from Google's view because it requires authentication to access. Meaning, it needs a username and password.

The easiest way to think about the Deep Web: It is all the data behind firewalls. Ex. databases, business intranets, web archives, password-protected websites, online banking or email account, direct messages on Twitter or photos uploaded to Facebook and marked private. Search engines cannot reach that content and a simple Google search of your name will not bring it into view.