DC Bar Webinar: June 3, 2020

Legal, Constitutional and Technological Challenges Presented by the Internet of Things and Emergent Technology Devices

Joel Schwarz

Managing Partner, The Schwarz Group LLC

TheSchwarzGroup@outlook.com

Adjunct Professor of Law, Albany Law School

jschw@albanylaw.edu

I. IoT Vulnerabilities

While IoT devices open up new worlds of convenience and enhance the quality of our lives in ways never before available - from watching your baby's vital signs from the office, to adjusting your home thermostat to the optimal level before you arrive home after a hard day's work- IoT devices have also introduced a number of new security vulnerabilities. At the risk of overgeneralizing, many of these vulnerabilities stem from the unique traits that make these singular-purpose IoT devices so attractive – simple to set-up and use – and thus, they tend to be basic and scaled down, with little if any internal memory, relying heavily on hardcoded attributes and firmware. And because manufacturers wish to make these available to the largest possible audience, by making them super simple to install and use - low "friction" in marketing-speak - they lack strong, if any, out of the box security, and often come with default accounts and passwords enabled; account names and passwords which are rarely, if ever, changed. The now infamous Mirai botnet attack in 2016 is an excellent illustrative example.

The Mirai attack began showing up on the radar of security professionals in August 2016, hitting its peak in September 2016. Interestingly, it was both a self-propagating worm, which replicated "itself by finding, attacking and infecting vulnerable IoT devices," as well as a botnet, because the IoT devices, once infected by Mirai, were "controlled via a central set of command and control (C&C) servers," the C&C servers being used to direct the infected IoT devices to the sites to attack next.[1] When all was said and done, the Mirai botnet was responsible for "record-breaking attacks" that crippled a number of high profile websites, despite the fact that the attack was "carried out via small, innocuous Internet-of-Things (IoT) devices like home routers, air-quality monitors, and personal surveillance cameras."[2] Perhaps most probative of our discussion about IoT device vulnerabilities is that the initial compromise of these devices "relied exclusively on a fixed set of 64 well-known default login/password combinations commonly used by IoT devices,"[3] meaning that it likely could have been avoided, had the owners of these devices merely changed, or disabled the default user IDs and passwords. Indeed, while this attack was very low tech, in terms of the exploit used, it proved extremely effective, leading to the compromise of over 600,000 IoT devices.[4]

Yet another vulnerability of IoT devices relates to how they are initialized when first installed. In the "old days" – "old" being a relative term- in order to install a new device, even one billed as "plug and play," you'd plug the device in, download driver updates, and then follow the instructions to install the device within your network, potentially needing to make changes to your security and firewall software, open ports through which the device would communicate home, etc. With at least some, if not many, IoT devices, however, there is no manual setup, and the device is available and accessible immediately, by virtue of its direct communication with the manufacturer. And therein lies the rub. They don't communicate through your network, but rather make a direct connection with the manufacturer using the peer-to-peer (P2P) network, jumping over your firewall, and circumventing traditional security protections enabled within your network.[5] Super simple to begin using, and

---

[1] *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis*, Dec 14, 2017, https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/amp/.
[2] *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis*, Dec 14, 2017, https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/amp/.
[3] *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis*, Dec 14, 2017, https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/amp/.
[4] *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis*, Dec 14, 2017, https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/amp/.
[5] *Consumers Urged to Junk Insecure IoT Devices*, Lindsey O'Donnell, June 18, 2019, Threat Post, https://threatpost.com/consumers-urged-to-junk-insecure-iot-devices/145800/

thus, low friction. Yet, by virtue of being plugged into your network, they open your network to attack and compromise. And for those unfamiliar with peer-to-peer networks, they are more difficult to trace since they are a direct connection between 2 "peers"/computers, and they therefore tend to be used by, although not exclusively, individuals who lack a respect for laws and are looking to conduct activities that may not be above-board. For example, intellectual property infringement thrives through the use of P2P to share cracked or otherwise copyrighted files.

On top of hopping outside your secured network and using the peer-to-peer protocol to phone back to the manufacturer, is the added security implications of manufacturers using the devices' physical serial number to individually track and communicate with the device. What that means is that if you know or can guess the serial number of the device, you can make a direct connection with the device. In such a scenario, a simple exploit to access and potentially co-opt an IoT device is to run a script trying various sequences of numbers until you hit upon a number(s) that represents the serial number of a particular IoT device (known as an "enumeration vulnerability"). You now have the ability to communicate directly with, and control, that device, without going through any firewalls, or potentially leaving any trace of this compromise.[6] And because the serial number of the device is hardcoded in, it cannot be changed, even once comprised.

Relatedly, the compromised IoT device then becomes a "pivot" point into all other parts of your network, and any devices connected to your network; i.e., the attacker might get in through a compromised IoT device, but might not actually be interested in the compromised camera or other IoT device itself. "[T]hey may go, oh, what other devices are on this network? So whether that's other computers or other IoT devices, then they can potentially keep on moving throughout the network. . . . this can very quickly escalate to other more serious things than spying on people."[7]

By way of an example, in April 2018, the CEO of cybersecurity company Darktrace "revealed that a casino fell victim to hackers thanks to a smart thermometer it was using to monitor the water of an aquarium they had installed in the lobby . . . The hackers managed to find and steal information from the casino's high-roller database through the thermometer," a database which "may have included information about some of the unnamed casino's biggest spenders along with other private details . . . . "[8] More recently, in August 2019 Microsoft announced that it had discovered attacks starting in April 2019 that targeted IoT devices – printers, video decoders and other devices – "as a beachhead to penetrate targeted computer networks."[9] Specifically, Microsoft researchers discovered that the attackers had breached the IoT devices and used them as a pivot point into the network through exploitation of device passwords that were "easily guessable default ones they shipped with," as well as through exploitation of devices "running an old firmware version with a known vulnerability."[10] Perhaps more alarming, Microsoft revealed that the perpetrators appeared to be a hacker

[6] *Consumers Urged to Junk Insecure IoT Devices*, Lindsey O'Donnell, June 18, 2019, Threat Post, https://threatpost.com/consumers-urged-to-junk-insecure-iot-devices/145800/

[7] *Consumers Urged to Junk Insecure IoT Devices*, Lindsey O'Donnell, June 18, 2019, Threat Post, https://threatpost.com/consumers-urged-to-junk-insecure-iot-devices/145800/

[8] *Hackers exploit casino's smart thermometer to steal database info*, Kellen Beck, Mashable, Apr 15, 2018, https://mashable.com/2018/04/15/casino-smart-thermometer-hacked/

[9] *Microsoft catches Russian state hackers using IoT devices to breach networks*, Dan Goodin, Aug 5, 2019, Ars Technica, https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/

[10] *Microsoft catches Russian state hackers using IoT devices to breach networks*, Dan Goodin, Aug 5, 2019, Ars Technica, https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/

group called "'Strontium,' a Russian government hacking group better known as Fancy Bear or APT28," which was also responsible for hacks into the "Democratic National Committee ahead of the 2016 presidential election," and "has also been linked to intrusions into the World Anti-Doping Agency in 2016, the German Bundestag, and France's TV5Monde TV station, among many others."[11]

Yet another IoT vulnerability stems from the limited internal memory of these devices, rendering them primarily, if not completely, dependent on manufacturer-installed firmware, which can only be overwritten by new firmware updates, limiting the options for additional, user-initiated security options. Relatedly, this opens up IoT devices to potential supply chain vulnerabilities. For example, as Finite State observed in its analysis of Huawei's IoT products, "[m]ost devices networked together in the Internet of Things (IoT), in fact, have too little memory to run security scanning software or anything else besides their purpose-built firmware."[12] Given this vulnerability, Finite State ran an automated script to search through firmware files embedded on IoT devices publicly accessible through the Internet, and within "a single 36-hour run . . . checked 1.5 million firmware files from 558 Huawei enterprise networking products — that's just business systems, not consumer devices — and found the average device had 102 vulnerabilities, at least a quarter of them severe enough to let a hacker get full access easily."[13]

The good news, to the extent there was any, is that that level of vulnerability is allegedly "much more than comparable Western products," so conceptually, one can avoid some of these IoT vulnerabilities by sticking with Western products.[14] The bad news, however, is that it's difficult if not impossible to differentiate where the IoT products originate from because "'white labeling' is extremely prevalent in the industry," meaning that manufacturers sell the product to a reseller, who then may resell it again, in either case relabeling it with their own brand, and thus masking the original brand and potential origin of the product.[15]

Privacy concerns, or the lack of privacy thereof, are yet another IoT vulnerability, as highlighted by a study conducted as a joint collaboration between Northeastern University and the Imperial College of London. In this study they took an in-depth look at 81 popular IoT devices, to include "smart TVs, streaming dongles, smart speakers, and video doorbells made by vendors including Google, Roku, and Amazon," finding that of those 81 devices, 72 "made contact with someone other than its manufacturer. In many instances, these transfers 'expose information to eavesdroppers via at least one plaintext flow, and a passive eavesdropper can reliably infer user and device behavior from the traffic . . . .'" [16] The personal information collected by these IoT devices

[11] *Microsoft catches Russian state hackers using IoT devices to breach networks*, Dan Goodin, Aug 5, 2019, Ars Technica, https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/

[12] *Hacker Heaven: Huawei's Hidden Back Doors Found*, Sydney J. Freedberg, Jr., July 5, 2019, Breaking Defense, https://breakingdefense.com/2019/07/hunting-huaweis-hidden-back-doors/

[13] *Hacker Heaven: Huawei's Hidden Back Doors Found*, Sydney J. Freedberg, Jr., July 5, 2019, Breaking Defense, https://breakingdefense.com/2019/07/hunting-huaweis-hidden-back-doors/

[14] *Hacker Heaven: Huawei's Hidden Back Doors Found*, Sydney J. Freedberg, Jr., July 5, 2019, Breaking Defense, https://breakingdefense.com/2019/07/hunting-huaweis-hidden-back-doors/

[15] *Consumers Urged to Junk Insecure IoT Devices*, Lindsey O'Donnell, June 18, 2019, Threat Post, https://threatpost.com/consumers-urged-to-junk-insecure-iot-devices/145800/

[16] *The Internet of Things Is Still a Privacy Dumpster Fire, Study Finds*, Karl Bode, Motherboard, Sept 19, 2019, https://www.vice.com/en_us/article/gyzjym/the-internet-of-things-is-still-a-privacy-dumpster-fire-study-finds

is also concerning, with the majority of IoT devices found to have "collected and shared information including your IP address, device specs (like MAC address), usage habits, and location data."[17]

Even more recently, researchers announced that voice-recognition IoT devices, such as Amazon Echo speakers, may be hackable using a simple laser or other light source. Specifically, a group of University of Michigan researchers announced that "[t]hey can now use lasers to silently 'speak' to any computer that receives voice commands - including smartphones, Amazon Echo speakers, Google Homes, and Facebook's Portal video chat devices" - by sending light commands, potentially from "hundreds of feet away," allowing them to "open car garages, make online purchases, and cause all manner of mischief or malevolence."[18]

According to the researchers, "'[i]t's possible to make microphones respond to light as if it were sound,'" meaning that "'anything that acts on sound commands will act on light commands.'"[19] While the precise reason for this ability is not yet fully understood, it appears that the microphone interprets the incoming light into a digital signal, just as it would a sound, perturbing the device's microphone membrane at the same frequency, and in the same manner, as the spoken word.[20] Just as worrisome, the researchers also claimed that they could use a laser beam to actually silence an IoT device, so that even if a person were home the voice assistant on the device would not provide an audibly discernable response alerting the owner that the device is being hacked.[21]

II. IoT Security

As noted above, IoT devices have a number of known security vulnerabilities, including:

- Failure to implement strong, if any, out of the box security;
- Shipping of devices with default accounts and passwords enabled (rarely, if ever changed);
- Use of the peer-to-peer (P2P) protocol to initialize, and then communicate with, the manufacturer, jumping over firewalls and circumventing network security;
- Shipping with hard coded device IDs that cannot be changed easily, if at all, even if compromised;
- Limited internal memory, rendering these devices primarily, if not completely, dependent on manufacturer-installed firmware, limiting options for additional, user-initiated security;
- Leakage of personal (sometimes sensitive) information, such as device usage habits and location data, to unknown parties, in many instances via plaintext, allowing a passive eavesdropper to intercept the content, to include the sensitive personal information; and
- Vulnerability of voice-recognition devices to remote hacking using a simple laser or other light source.

Given that the Internet grew up organically, with the initial focus being to convince people to trust and adopt the new technology, one might almost forgive Internet providers, computer manufacturers and old-world companies for being remiss in not incorporating security from the start. IoT devices, on the other hand, don't

[17] *The Internet of Things Is Still a Privacy Dumpster Fire, Study Finds*, Karl Bode, Motherboard, Sept 19, 2019, https://www.vice.com/en_us/article/gyzjym/the-internet-of-things-is-still-a-privacy-dumpster-fire-study-finds
[18] *Hackers Can Use Lasers to 'Speak' to Your Amazon Echo or Google Home*, Andy Greenberg, Wired Magazine, Nov. 4, 2019, https://www.wired.com/story/lasers-hack-amazon-echo-google-home/.
[19] *Hackers Can Use Lasers to 'Speak' to Your Amazon Echo or Google Home*, Andy Greenberg, Wired Magazine, Nov. 4, 2019, https://www.wired.com/story/lasers-hack-amazon-echo-google-home/.
[20] *Hackers Can Use Lasers to 'Speak' to Your Amazon Echo or Google Home*, Andy Greenberg, Wired Magazine, Nov. 4, 2019, https://www.wired.com/story/lasers-hack-amazon-echo-google-home/.
[21] *Hackers Can Use Lasers to 'Speak' to Your Amazon Echo or Google Home*, Andy Greenberg, Wired Magazine, Nov. 4, 2019, https://www.wired.com/story/lasers-hack-amazon-echo-google-home/.

have such excuse. Well before the first Internet connected thermostat ever hit the market, and before the first Internet-connected refrigerator advertisement aired, we were all well aware of the cybersecurity and privacy challenges posed by IoT devices, and the potential vulnerabilities they introduced. But the race for IoT market share and consumer adoption trumped security.

Interestingly, this isn't dissimilar from the late 1990's, when online trading became all the rage. Back then, brokerage firms began offering online trading, day-trading from home became an attractive and viable career option, and the public was able to access IPOs previously reserved for financial market insiders and the well connected, cumulatively causing a massive influx of online customers. This in turn led to widespread brokerage website outages and consumer complaints, as stocks quickly moved and people were unable to get into their online accounts to sell their shares and cut their losses, or cash in on a quick profit, leading to investigations of the industry by regulators, such as the New York State Attorney General's Office.[22]

Inevitably, one of the primary causes of these outages was that brokerage firms were all rushing in to gain market share, well before they had the capacity to deal with that market share. In other words, market share trumped all other considerations, not unlike the mindset of IoT device makers today when it comes to building in appropriate security. Even with a plethora of IoT devices regularly hitting the market, there's still a lack of any wide-spread incorporation of security by manufacturers.

For example, in 2017 the European Union Agency for Cybersecurity published its 'Baseline Security Recommendations for IoT,' followed by multiple publications providing guidance on various IoT security requirements . . . ."[23] And in August 2019, the U.S. National Institute of Standards and Technology (NIST) offered special guidance for securing IoT devices in its first draft of a "Core Cybersecurity Feature Baseline for Securable IoT Devices," which followed on the heels of its June publication, "Considerations for Managing Internet of Things cybersecurity and Privacy Risks."[24] And of course, the NIST Cybersecurity Framework, which dates back to 2013 (when the initial draft was first published), could also be helpful to IoT Device manufacturers, were they interested in integrating cybersecurity and privacy "by design."

Perhaps because of the dearth of progress towards securing IoT devices through self-regulation, governments and regulators have begun taking matters into their own hands, leading to a spate of IoT-specific security laws being enacted. In the U.S., one of the first of those was the California IoT law, which went into effect on January 1, 2020, having been described as a "first of its kind" law that will "create significant compliance obligations for organizations across a broad range of sectors."[25] The California IoT law applies to organizations that manufacture Internet connected devices "sold or offered for sale in California," potentially covering a wide range of devices and objects capable of Internet connectivity, so long as they are assigned an IP address or Bluetooth address.[26] Most relevant to this discussion, the law requires device manufacturers to equip each connected device "with a reasonable security feature or features . . . appropriate to the nature and function of

[22] *From Wall Street to Web Street: A Report on The Problems and Promise of the Online Brokerage Industry*, New York State Attorney General's Office, Nov 22, 1999, http://www.joelschwarz.com/AGSiteDocs/OBSReportFull.pdf
[23] *Are you prepped for the influx of IoT security laws? It starts in Calif.*, Darcy Brosky and Steven Stransky, IAPP, Nov 26, 2019, https://iapp.org/news/a/are-you-prepped-for-the-influx-of-iot-security-laws-it-starts-in-california/#
[24] *Are you prepped for the influx of IoT security laws? It starts in Calif.*, Darcy Brosky and Steven Stransky, IAPP, Nov 26, 2019, https://iapp.org/news/a/are-you-prepped-for-the-influx-of-iot-security-laws-it-starts-in-california/#
[25] *Are you prepped for the influx of IoT security laws? It starts in Calif.*, Darcy Brosky and Steven Stransky, IAPP, Nov 26, 2019, https://iapp.org/news/a/are-you-prepped-for-the-influx-of-iot-security-laws-it-starts-in-california/#
[26] *Are you prepped for the influx of IoT security laws? It starts in Calif.*, Darcy Brosky and Steven Stransky, IAPP, Nov 26, 2019, https://iapp.org/news/a/are-you-prepped-for-the-influx-of-iot-security-laws-it-starts-in-california/#

the device, appropriate to the information the device may collect, contain or transmit [and] [d]esigned to protect both the device and any information it contains . . . ."[27] While the precise meaning of "reasonable security" is left undefined – and thus ripe for litigation by regulators and consumers' attorneys - the law does clarify that the "reasonable security" requirement is presumed to be satisfied if the IoT device is equipped with a "means for **authentication** outside a local area network" and utilizes a "unique password" or requires some other type of **secure authentication** before access to the device is granted the first time.[28]

Other countries have also begun focusing on IoT security mandates. For example, in May 2019, the UK announced its plans to introduce an IoT security law for IoT manufacturers requiring mandatory security labeling, with the penalty for non-conformance being getting barred from selling IoT devices within the country.[29]

But at the end of the day, the path to better IoT security really isn't a mystery. Given the known vulnerabilities, the path is pretty clear, and includes:

- shipping all IoT devices with default accounts and passwords disabled;
- the use of identification and authentication protocols when allowing access to an IoT device;
- a process for reconfiguring IoT device security when needed or desired (for example, as noted above, hardcoded device IDs currently prevent the ability to change those IDs, even once compromised);
- limiting access to local and approved network interfaces (addressing some of the unsanctioned P2P connections by IoT devices discussed above);
- encryption of all communications between the IoT device and the manufacturer/authorized user;
- requiring secure software and firmware updates;
- locking down the parties with whom the device communicates, limiting this to only the manufacturer and the authorized user; and
- requiring devices to utilize security incident logging, which would allow us to trace the source of a compromise of an IoT device, or devices.[30]

III. Highly sensitive data used in criminal prosecution cases

As much as the ubiquity of IoT devices in our daily lives has given rise to an ongoing debate about the proper legal standard for allowing law enforcement access to the records that they collect, sometimes no legal process at all is needed. A prime example is the Ring doorbell/camera device, which, as a Ring representative told Senators in November 2019, may be made available to police and other law enforcement – roughly 630 law enforcement agencies as of the end of 2019 - without providing any evidence of a crime; and this data may be

[27] *Are you prepped for the influx of IoT security laws? It starts in Calif.*, Darcy Brosky and Steven Stransky, IAPP, Nov 26, 2019, https://iapp.org/news/a/are-you-prepped-for-the-influx-of-iot-security-laws-it-starts-in-california/#
[28] *Are you prepped for the influx of IoT security laws? It starts in Calif.*, Darcy Brosky and Steven Stransky, IAPP, Nov 26, 2019, https://iapp.org/news/a/are-you-prepped-for-the-influx-of-iot-security-laws-it-starts-in-california/# (emphasis added).
[29] *Are you prepped for the influx of IoT security laws? It starts in Calif.*, Darcy Brosky and Steven Stransky, IAPP, Nov 26, 2019, https://iapp.org/news/a/are-you-prepped-for-the-influx-of-iot-security-laws-it-starts-in-california/#
[30] *Are you prepped for the influx of IoT security laws? It starts in Calif.*, Darcy Brosky and Steven Stransky, IAPP, Nov 26, 2019, https://iapp.org/news/a/are-you-prepped-for-the-influx-of-iot-security-laws-it-starts-in-california/#

retained indefinitely by the recipient.[31] Indeed, police can request "up to 12 hours of video from anyone within a half square mile of a suspected crime scene, covering a 45-day time span," with nothing more than "a case number for the crime they are investigating, but not any other details or evidence related to the crime or their request."[32]

Of course, for those familiar with recent Supreme Court decisions regarding law enforcement access to personal data collected by, or from, electronic devices, one might wonder how police can gain access to 45 days-worth of Ring device records without any legal process whatsoever? For example, in Carpenter v. U.S., the Supreme Court required use of a search warrant for law enforcement access to over a month of cell-site location records identifying Carpenter's whereabouts, because the combined result of accessing records collected over a period of time provides a "comprehensive dossier of [] physical movements" - an "intimate window into a person's life" – enabling law enforcement to track, monitor and surveil someone in a way that was never before practicable.[33] Similarly, one might expect that 45 days of Ring video records would also be protected from law enforcement access without a warrant, for similar reasons.

There are actually three (3) reasons, however, why Ring can potentially disclose these records to law enforcement without legal process. First, and foremost, the owners of Ring devices are apparently making the data available to police and other law enforcement by consenting to its use and disclosure when joining "Ring's Neighbors social network," as well as when individual police access requests for video are received.[34] As Ring noted to the Senate, Ring "does not own or otherwise control users' videos," as they "intentionally designed the Neighbors Portal to ensure that users get to decide whether to voluntarily provide their videos to the police."[35]

Second, because the information accessed by law enforcement comes from the devices of 3rd parties – the Ring devices being nothing more than electronic witnesses that happen to be at the right place, at the right time – it's questionable whether defendants would even be able to legally challenge law enforcement access to these records. In Carpenter, he was able to challenge access to *his* cell site location records because those records were collected from *his* cell phone, and thus he was able to assert a 4th Amendment expectation of privacy in his cellphone and the records it generated. By contrast, a defendant concerned about the release of Ring records would be unlikely to be in the position to claim a 4th Amendment reasonable expectation of privacy, because the records come from a device owned by an uninvolved 3rd party, and it would not be reasonable for a defendant to claim an expectation of privacy in records he may or may not even know exist, and which are generated when he visits a 3rd party's property.

---

[31] *Police can keep Ring camera video forever and share with whomever they'd like, Amazon tells senator*, Drew Harwell, Washington Post, Nov 19, 2019, https://www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator/

[32] *Police can keep Ring camera video forever and share with whomever they'd like, Amazon tells senator*, Drew Harwell, Washington Post, Nov 19, 2019, https://www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator/

[33] Carpenter v. U.S., No. 16-402, 585 U.S. ____ @ 12-13, 17 (2018)

[34] *Police can keep Ring camera video forever and share with whomever they'd like, Amazon tells senator*, Drew Harwell, Washington Post, Nov 19, 2019, https://www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator/

[35] *Police can keep Ring camera video forever and share with whomever they'd like, Amazon tells senator*, Drew Harwell, Washington Post, Nov 19, 2019, https://www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator/

Finally, although Ring's terms of service state that users are required to install these cameras so that they do not record past a person's home boundary, these devices have nonetheless been known to record outwards, capturing activity on public roads or sidewalks (or the front stoop of a person's house). By capturing activity within the public view, it's unlikely that the actions captured would be protected, because under 4th Amendment jurisprudence, it would be unreasonable to expect privacy in actions that occur in a public space (although admittedly, the D.C. Circuit Court's decision in U.S. v. Maynard,[36] the Supreme Court's decision in U.S. v. Jones (specifically, the concurring opinions of Justice Sotomayor[37] and Alito[38]), and the Supreme Court's decision in Carpenter v. U.S.,[39] did open the door to questioning whether actions in the public view, captured over an extended period of time, are due some 4th Amendment protection).

Of course, as Ring has publicly stated, users are permitted to decline police requests for video footage or opt out of the Neighbor's social network. It's unclear, however, how widely this right is exercised, how much attention average consumers pay to this option, and/or whether the average consumer even understands what their choices are. In other words, its arguable whether manufacturers have done enough to address consumer awareness of the security/privacy options, and thus, how much consumers are able to protect themselves and exercise knowing consent (or revoke that consent).

IV. Unique 4th Amendment IoT Challenges: Airbags and Embedded Car Sensors

Coupled with the growing prevalence of IoT devices and technology throughout our homes and offices, today we're also seeing an increasing prevalence of technology in our vehicles. From devices used by rental car and insurance companies for monitoring driving activity, to tech that controls our vehicle's climate, self-driving or semi-autonomous modes of operation, to safety systems (including airbags) that monitor vehicles immediately before and up to a crash (akin to the black-boxes used in planes). Unlike traditional IoT devices, however, which rely upon Internet connectivity to exchange information with a 3rd party provider (storing data with the provider, or in the Cloud), the data captured by these airbag devices generally remains within the device itself, inside the vehicle, albeit difficult to access and decipher. Given the local storage of this data, the accessing and downloading of this data by law enforcement or other governmental agencies, after an accident, has given rise to questions about whether the 4th Amendment right to privacy applies to the data on these devices. This has, in turn, led to a divergence of opinions in the few states that have considered this question to date.

a. California: People v. Diaz (2013)

In People v. Diaz,[40] Elva Diaz drove home after a night of drinking, with a blood alcohol level of .20, approximately 2 ½ hours after the accident (meaning that her blood alcohol was approximately .23 at the time

[36] 615 F.3d 544 (D.C. Cir. 2010).
[37] 565 U.S. 400, 413 (2012).
[38] 565 U.S. 400, 430 (2012).
[39] No. 16-402, 585 U.S. ____ (2018).
[40] 213 Cal. App. 4th 743 (State of California 2013), https://www.leagle.com/decision/incaco20130206055.

of the accident), crossed over the double yellow lines on a highway, and collided head-on with another vehicle, killing the driver of the other vehicle and coming to rest upside down, on the other side of the road.[41] Diaz's vehicle was subsequently impounded by the California Highway Patrol (CHP) and, without a search warrant, the CHP's Multidisciplinary Accident Investigation Team put the vehicle through a thorough inspection, including downloading the vehicle's control modules, to include the Sensing Diagnostic Module (SDM); the SDM's main function being to deploy the air bags, with the secondary function being to record "throttle, speed, application of brakes, and transmission position."[42] Diaz was subsequently charged with involuntary manslaughter and the lesser included offense of second degree murder, as well as vehicular manslaughter with gross negligence while intoxicated.

Before trial, Diaz moved to suppress the data seized from her impounded vehicle's SDM, arguing that the warrantless search and seizure of the SDM violated her 4th Amendment rights. Specifically, she argued that "because the SDM was inaccessible and not in plain view, and its data were unavailable without connecting the SDM to a computer," she had a constitutionally-protected REP in the data, "even if she herself did not know of the presence of the SDM."[43] The trial court held a hearing on the motion, at which time a Sergeant from CHP testified that "the SDM is included in the mechanical inspection of the vehicle because 'it's an intricate [sic., integral] component of the vehicle no different than a master cylinder," and thus "[i]t was standard protocol to download the 'black box'" without a court order, because "the SDM data . . . corroborates data the investigators look at when they check brakes, acceleration, and the steering column."[44]

After hearing arguments from both sides, the trial court ruled that that there was no 4th Amendment protection for the SDM data, because the defendant "had no subjective belief in . . . a privacy interest in an SDM that she probably didn't know existed."[45] As a result, the court denied her suppression motion. The court further noted that even if the defendant had been aware of the SDM, she wouldn't have had an REP in the data on it because SDMs do not "gather any personal information." [46] Further, the court found that the defendant could have "no reasonable expectation of privacy in her speed on a public roadway or when and if she applied her brakes shortly before the crash" - the type of data gathered by an SDM – because "if a witness had observed those actions and testified to them, the evidence would be admitted." [47] By analogy, the court noted that the SDM is

[41] 213 Cal. App. 4th @ 746-748.
[42] 213 Cal. App. 4th @748.
[43] 213 Cal. App. 4th @ 750.
[44] 213 Cal. App. 4th @ 751.
[45] 213 Cal. App. 4th @ 752.
[46] 213 Cal. App. 4th 752.
[47] 213 Cal. App. 4th 752.

merely an "electronic witness" whose testimony is also admissible as to actions occurring in public view.[48] Diaz was subsequently found guilty by jury of involuntary manslaughter and vehicular manslaughter with gross negligence while intoxicated, which she appealed to the California Appellate Division.

In the absence of precedent, the Appellate Court looked to other cases relating to warrantless searches of impounded vehicles, noting that "[w]hen the police lawfully seize a car which is itself evidence of a crime, rather than merely a container of incriminating articles, they may postpone searching it until arrival at a time and place in which the examination can be performed in accordance with sound scientific procedures."[49] Looking to a more recent California case, the Appellate Court noted that when officers seize a vehicle incident to an arrest, pursuant to a "'reasonable belief that the object is itself evidence of the commission of the crime for which the arrest is made, any subsequent examination of the object for the purpose of determining its evidentiary value does not constitute a 'search' as the term is used in the California and federal Constitutions.'"[50] The Appellate Court then pointed out that Diaz's vehicle was itself an instrumentality of the crime of vehicular manslaughter, which she had previously conceded was lawfully seized. As such, "the search . . . fell squarely within the instrumentality exception to the warrant requirement."[51]

Interestingly, Diaz cited to the Supreme Court's decision in U.S. v. Jones in challenging the warrantless search/seizure of the SDM data from her impounded vehicle. Specifically, in U.S. v. Jones, the FBI was accused of placing a GPS tracker on Jones' vehicle, without a valid search warrant, collecting precise positioning information about the vehicle over the course of close to a month. Notably, the FBI only turned on the device when the vehicle was in public spaces – i.e., they did not track the vehicle when it was in presumably private spaces such as a garage – therefore arguing that all of the information gathered was done while in public view, where there was no REP. Inevitably, however, the majority in the *Jones* case agreed that a search warrant was necessary because the GPS device was initially placed on the vehicle while on private property, violating the 4th Amendment by "trespassing" on private property.

While concurring with the majority's decision, however, Justice Sotomayer expressed 4th Amendment concerns that went beyond the mere concept of trespass. Specifically, she was concerned about warrantless GPS tracking of the vehicle over an extended period of time because the conglomeration of close to a month of precise GPS information paints an intricate portrait of a person's life – one that would not previously have been available

[48] 213 Cal. App. 4th 752.
[49] 213 Cal. App. 4th @ 755 (quoting People v. Teale, 70 Cal.2d 497 (1969)).
[50] 213 Cal. App. 4th @ 755 (quoting People v. Rogers. 2 Cal.3d 542 (1978)).
[51] 213 Cal. App. 4th @ 756-757.

absent modern technology - which she believed should be protected by the 4th Amendment.[52] By analogy, Diaz argued that because SDMs also collect a great deal of information about the actions of the driver and the vehicle, they paint an intricate picture of the driver's actions, which by the same logic that Sotomayor used in *Jones*, should render the SDM data 4th Amendment protected (thus requiring a search warrant before searching).[53]

The California Appellate Court dismissed this argument, however, noting that the purpose of the SDM device involved here was not installed to obtain information for the police, unlike the GPS tracker in the *Jones* case (as the device was installed by the car manufacturer).[54] The California Appellate Court therefore concluded that there was no 4th Amendment REP in the SDM data, and thus, no violation when the police conducted a warrantless search and seizure of the device's data from Diaz's vehicle.[55] The Court bolstered this holding by observing that "a person has no reasonable expectation of privacy in speed on a public highway because speed may readily be observed and measured through, for example, radar devices . . . or estimation by a trained expert. Similarly, a person has no reasonable expectation of privacy in use of a vehicle's brakes because statutorily required brake lights . . . announce that use to the public. Thus, defendant has not demonstrated that she had a subjective expectation of privacy in the SDM's recorded data . . . technology merely captured information defendant knowingly exposed to the public."[56]

b. **Florida: State of Florida v. Worsham (2017)**

On October 6, 2013, Charles Worsham was involved in a high-speed crash that killed his passenger, after which his car was impounded.[57] On October 18th, 12 days after the crash, the police accessed Worsham's impounded vehicle and downloaded data from the vehicle's event data recorder ("EDR") without a warrant.[58] Worsham was subsequently charged with DUI manslaughter and vehicular homicide.

---

[52] U.S. v. Jones, 565 U.S. 400, 415-416 (2012), quoting Sotomayor, J., concurring. Specifically, Justice Sotomayor stated that "I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated . . . ." U.S. v. Jones, 565 U.S. @ 415-416 (2012).
[53] 213 Cal. App. 4th @ 757.
[54] 213 Cal. App. 4th @ 757.
[55] 213 Cal. App. 4th @ 758.
[56] 213 Cal. App. 4th @ 757.
[57] State of Florida v. Worsham, 227 So.3d 602, 603 (4th District 2017), https://www.leagle.com/decision/inflco20170329178.
[58] 227 So.3d @ 603.

At trial, Worsham moved to suppress the evidence from the EDR, arguing that he had a 4th Amendment REP in the information, and thus downloading the data without a warrant violated his 4th Amendment rights.[59] The trial court agreed, granting Worsham's motion to suppress the evidence, and the State appealed.

On appeal, the Florida Appellate Court began by reviewing U.S. Supreme Court precedent, noting that "even where . . . information is accessible to the public," it may still be constitutionally protected; "[t]his is why 'a car's interior as a whole is . . . subject to Fourth Amendment protection from unreasonable intrusions by the police.'"[60] Citing to more recent Supreme Court precedent, *Riley v. California*, the Florida Appellate Court observed that the Supreme Court has prohibited the search of an arrestee's cell phone incident to arrest, despite the long-established principle that permits the police to conduct a warrantless search of an arrestee, as well as all items found on his person. Specifically, the Supreme Court in *Riley* held that upon balancing the individual's privacy interest in his cell phone, given the amount of personal information on the phone, against the governmental interest in warrantless searching and seizure of items from an arrestee's person during an arrest, the balance tips in favor of the arrestee, because the reasons for permitting a warrantless search incident to arrest are officer safety and protection, neither of which are significantly furthered through seizure of a cell phone (the privacy interests impacted by searching an arrestee's cell phone being significant).[61] the Florida Appellate Court then went on to note that a "car's black box is analogous to other electronic storage devices for which courts have recognized a reasonable expectation of privacy," and that "[t]he emerging trend is to require a warrant to search these devices."[62] The court also highlighted a 2011 Florida Supreme Court precedent, which distinguished between "computer-like electronic storage devices" and more traditional "inanimate objects," because computers hold such a vast amount of personal and sensitive information touching on many aspects of a person's private life, thus creating "a far greater potential for . . . a consequent invasion of privacy when police execute a search for evidence on a computer."[63]

Because this was a question of first impression in Florida, the court began by reviewing the evolution of these airbag safety devices, and their unique characteristics, noting that EDRs are installed in about 96% of cars manufactured after 2013, and are designed to record "'crash data or technical vehicle and occupant information for a period of time before, during and after a crash," activating during an event, or recording information on a continuous loop, until a vehicle is in a crash.[64] Indeed, "[t]he National Highway Traffic Safety Administration has

[59] 227 So.3d @603.
[60] 227 So.3d @604 (quoting Katz v. United States, 88 S.Ct. 507 (1967), and New York v. Class, 475 U.S. 106 (1986)).
[61] 816 S.E.2d @ 773.
[62] 227 So.3d @ 604 (quoting Riley v. California, __ U.S. __ (__).
[63] 227 So.3d 604-605 (quoting U.S. v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011).
[64] 227 So.3d @605-606.

standardized the minimum requirements for electronic data recorders, mandating that the device record 15 specific data inputs, including braking, stability control engagement, ignition cycle, engine rpm, steering, and the severity and duration of a crash . . . [a]long with these required data inputs, the devices may record additional information like location or cruise control status and some devices can even perform diagnostic examinations to determine whether the vehicle's systems are operating properly."[65] The Court then went on to observe that the data is difficult to retrieve, requires a special retrieval kit that is both expensive and manufacturer-specific, and that the data, once retrieved, must still be interpreted by a specially-trained investigator.[66] Likewise, the Court noted that the EDR in this case captured a wide range of data that is materially different from the traditional items a mechanic might have access to when "putting a car on a lift and examining the brakes or tires."[67]

Because of the inherent difficulty in accessing EDR data, the specialized skills needed to interpret the data, and the array of detailed data, "different from the tangible 'mechanical' parts of a vehicle," the Florida Appellate Court held that there is a 4th Amendment Reasonable Expectation of Privacy in the EDR information, and a search warrant was therefore required.[68] In reaching this conclusion, the court placed weight on the fact that EDRs document more than what is voluntarily conveyed to the public.[69] The Court also pointed to the Driver Privacy Act of 2015 for support, a federal law enacted after the accident, which states that "[a]ny data retained by an event data recorder . . . is the property of the owner . . . of the motor vehicle in which the event data recorder is installed," and in general, "may not be accessed by a person other than an owner . . . of the motor vehicle in which" installed.[70] Indeed, passage of this Act was key to the court distinguishing its holding in this case from the holding of the California state court in People v. Diaz, the statute having been passed after the Diaz decision.[71]

Interestingly, a well-reasoned dissent offered 5 reasons why the majority was incorrect in finding a 4th Amendment REP in the EDR data. Specifically, the dissent noted that there could be no REP in this data because "it is likely that Appellee did not even know that the vehicle he was driving had an EDR. Therefore, it would be quite a stretch to conclude that Appellee sought to preserve this information as 'private.'"[72] Second, to the extent the majority tried to analogize a cell phone to an EDR device in order to find support in the Riley v.

[65] 227 So.3d @606.
[66] 227 So.3d @606.
[67] 227 So.3d @606.
[68] 227 So.3d @606.
[69] 227 So.3d @606.
[70] 227 So.3d @607 (quoting The Driver Privacy Act of 2015, 49 U.S.C. §§30101 note, 24302(a) (2015)).
[71] 227 So.3d @607.
[72] 227 So.3d @609.

California Supreme Court case, the dissent argued that these two devices are worlds apart, in that an EDR is "attached to an undercarriage of a motor vehicle" and contains "extremely non-private, non-confidential information, such as the vehicle's yaw rate," while cell phones are carried close to an individual's body, and contain personal, distinctive and sensitive information that reveals "much more in combination than an isolated record."[73] Third, "[t]he private data in a cell phone is, for the most part, created by the owner and is password protected by the owner for his/her own benefit and privacy. The data on the EDR, however, was not created by the owner and was not protected by a password by or for the benefit of the owner . . . . "[74] Fourth, quoting from the Diaz court in California, the dissent argued that there can be no REP in an EDR because the technology "merely captured information defendant knowingly exposed to the public . . . ."[75] Finally, addressing the Driver Privacy Act of 2015 cited by the majority in support of an REP, the dissent downplayed the significance of this statute, noting that the statute was passed to provide guidance to owners and car manufacturers vis-à-vis ownership of the data on the device, as between those 2 parties, not to itself create a constitutionally-protected REP . . . ."[76] As a result, because "the data was not personal to Appellee, was not password protected by Appellee, and was not being collected and maintained solely for the benefit of Appellee," the dissent argued that there was no 4th Amendment protection for this data. [77]

Nonetheless, the majority opinion in this case held that the trial court was correct in finding a 4th Amendment REP in the data on the EDR, and thus, suppression of the data retrieved from the EDR was appropriate.[78]

c. **Georgia: Mobley v. State (2018 and 2019)**

Finally, the State of Georgia recently jumped into the fray when it decided Mobley v. State, after Mobley collided with a vehicle that was pulling out onto the road from a private driveway, resulting in the death of the 2 people in that vehicle.[79] Shortly after the accident, while still on scene, the police accessed and downloaded the data from Mobley's vehicle's Airbag Control Module (ACM), without a warrant. This information was subsequently used in the prosecution of Mobley for reckless driving and 2 counts of homicide by vehicle.[80] Before trial, Mobley moved to suppress this information, arguing that the police needed a search warrant to download and access the data from the ACM, and in the absence of such warrant, use of the evidence violated

[73] 227 So.3d @609-610 (quoting Riley v. California, ___ U.S. ____ (2014)).
[74] 227 So.3d @610.
[75] 227 So.3d @610.
[76] 227 So.3d @611.
[77] 227 So.3d @611-612.
[78] 227 So.3d @606.
[79] 816 S.E.2d 769 (Georgia Court of Appeals 2018), https://www.leagle.com/decision/ingaco20180627225.
[80] 816 S.E.2d @ 771.

his 4th amendment rights and should be suppressed. The trial court denied Mobley's motion to suppress, and Mobley appealed to the Court of Appeals of Georgia.

In support of his motion to suppress, Mobley cited the Supreme Court's decision in *U.S. v. Riley*, holding that an individual arrestee's privacy interest in his cell phone outweighs any governmental interest in warrantless searching of the phone at the time of arrest, given the amount of personal information people store on their cellphones today.[81] By analogy, Mobley argued that given the amount of information captured by an ACM,[82] the court should apply the 4th Amendment here as well, requiring a search warrant in order for law enforcement to gain access to the ACM data.

Nonetheless, the Court of Appeals distinguished the Riley case, stating that "[i]nformation regarding the mechanical functioning of the vehicle and its systems is qualitatively different from photographs, financial information, and other such personal data that may be found on a cell phone."[83] Cognizant of the Supreme Court's evolving perspective on the 4th Amendment implications of tracking a person's location, the Georgia Court of Appeals also considered and dismissed Justice Sotomayor's concurring opinion in the *Jones* GPS case, noting that unlike "the precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual association," the information collected by the ACM was not "capable of GPS monitoring or the recording of his movements between various locations."[84] Nor did the ACM collect information on a long term, extended basis – as was the focus in the *Jones* case - because "the ACM only starts recording information when an event, such as a collision, 'triggers' it to record."[85]

In dismissing Mobley's argument and ruling that he had no REP in this data, the Court of appeals found that the ACM device merely collected information **already exposed to the public** (albeit in a more detailed manner), such as the driver's approximate speed, when he hit his brakes in reference to the accident, etc. all of which he knowingly exposes to the public, and which people outside the vehicle could/would witness.[86]

Georgia Court of Appeals Chief Judge Dillard issued a concurring opinion, agreeing that the evidence should not be suppressed. But such agreement was based upon a legal doctrine known as the "inevitable discovery"

[81] 816 S.E.2d @ 773.
[82] For example, ACM data collection includes "the status of several aspects of the vehicle at or immediately preceding airbag deployment, including speed, engine speed, brake status, throttle position, engine revolutions, driver's seat belt status and brake switch status . . . and diagnostic information on the vehicle's systems." 816 S.E.2d @ 772.
[83] 816 S.E.2d @ 774.
[84] 816 S.E.2d @ 774.
[85] 816 S.E.2d @ 774.
[86] 816 S.E.2d @ 774.

doctrine, "which 'allows admission of evidence that was discovered as a result of police error or misconduct if the State establishes by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means without reference to the police error or misconduct.'"[87] Specifically, the Chief Judge noted that one officer had testified that had the ACM data not been obtained at the scene of the accident, "he would have sought a search warrant and collected such data from the vehicle at the impound lot."[88] Thus, the ACM data would have inevitably been discovered, and it was "unnecessary for us to address whether the Fourth Amendment prohibits a warrantless seizure of the data."[89]

After losing at the Court of Appeals, the case made its way up to the Georgia Supreme Court, which reversed, ruling that the ACM data was in fact protected by the 4th Amendment, and that the data should therefore have been suppressed, and not admitted against Mobley at his trial. Specifically, the Georgia Supreme Court noted that the question of whether the government has intruded into a private sphere where a person has a Reasonable Expectation of Privacy is not the only test for whether a 4th Amendment protected search and seizure has taken place. Rather, the Reasonable Expectation of Privacy test is **in addition to**, **not a substitute for**, the common law trespass analysis under the 4th Amendment, which looks to whether the government has trespassed on a person's house, papers, or "effects."[90] And in this particular case, the Georgia Supreme Court noted that "[a] personal motor vehicle is plainly among the 'effects' with which the Fourth Amendment . . . is concerned. . . . "[91] Thus, because the search of Mobley's vehicle was a "physical intrusion . . . for the purpose of obtaining information for a law enforcement investigation," this constituted a search, under the traditional 4th amendment principal of common law trespass.[92] And without a warrant, or an exigent circumstance necessitating an immediate search without a warrant, the search of the ACM in Mobley's vehicle was "an unreasonable search and seizure that violated the Fourth Amendment."[93]

In reaching this conclusion, the Georgia Supreme Court considered, but dismissed, the "inevitable discovery doctrine," because there was no evidence in the record that the officers were "'actively pursu[ing]'" a search warrant at the time that the data was downloaded from Mobley's vehicle, at the collision site.[94] Moreover, the court dismissed the relevance of an officer securing a search warrant the *following day*, after seizing the ACM

[87] 816 S.E.2d @ 775.
[88] 816 S.E.2d @ 775.
[89] 816 S.E.2d @ 775.
[90] Mobley v. The State, S18G1546 (Georgia Sup Ct Oct 21, 2019) @ 15.
[91] Mobley v. The State, S18G1546 (Georgia Sup Ct Oct 21, 2019) @ 16.
[92] Mobley v. The State, S18G1546 (Georgia Sup Ct Oct 21, 2019) @ 16.
[93] Mobley v. The State, S18G1546 (Georgia Sup Ct Oct 21, 2019) @ 18-19.
[94] Mobley v. The State, S18G1546 (Georgia Sup Ct Oct 21, 2019) @ 38 (quoting from the record in the case).

data from Mobley's vehicle, because "'a valid search warrant nearly always can be obtained after a search has occurred' [and] allowing law enforcement to use a warrant from after-the-fact to justify an earlier search would threaten to vitiate the warrant requirement."[95]

As such, the Georgia Supreme Court determined that the trial court should have granted Mobley's motion to suppress the evidence seized from his vehicle's ACM at the crash site, because downloading of that data without first securing a search warrant was a violation of his 4th Amendment rights.[96]

d. Vehicle-Based Safety Devices and the 4th Amendment: Where Do We Go From Here?

For those keeping score, we now have 2 states that have found 4th Amendment protection for the data stored on a vehicle's airbag deployment system, and 1 state that has found no 4th Amendment protection in such data. Inevitably, more states will likely have to wade into this question, so the issue is by no means settled. Yet in reviewing these cases, there appear to be 3 areas where the courts lack consensus, and thus with which they have wrestled when assessing whether there is a 4th Amendment REP in the data stored on these devices.

The first question is whether the person was even aware of the fact that there was a device in the vehicle collecting this information in the first place. According to the *Diaz Court*, apparently a person cannot have an REP in a device that they are completely unaware of. This was likewise cited by the dissent in the *Worsham* case. While this might make sense from a lay person's perspective – after all, how can you have any expectation, including a privacy expectation, if you don't even know something exists - this seems like a dangerous path to pursue in the context of the 4th Amendment. To illustrate, we can envision a couple building a new home. They tell the builder that they want high-speed Internet in every room of the house, the ability to play music anywhere in the house or backyard, and the ability to control the lights and thermostat remotely, over the Internet. In order to meet these requirements, the builder (or a subcontractor) installs the tech needed, potentially including high-speed ethernet or HDMI cabling inside the walls to a central junction box somewhere in the house, installation of wireless repeaters in various parts of the house, installation of blue tooth-enabled IoT devices throughout the house, such as lights and speakers, as well as installation of a Nest thermostat (or similar equipment) for purposes of monitoring and controlling the environment remotely. But, depending on the level of technological sophistication of the couple, they may have little to no awareness of what devices are needed, or installed. And at the end of the day, it probably doesn't matter. So long as they have their amenities, they're happy. And while it's true that they might receive manuals about these devices

[95] Mobley v. The State, S18G1546 (Georgia Sup Ct Oct 21, 2019) @ 38-39 (quoting U.S. v. Satterfield, 743 F.2d 827, 846 (11th Cir. 1984).
[96] Mobley v. The State, S18G1546 (Georgia Sup Ct Oct 21, 2019) @ 41-42.

when they take possession of the home, they may not read these manuals, any more so than a new car purchaser reads the voluminous manuals that come with the car (which presumptively contain information about the airbag safety device installed in the vehicle). The point here is that the couple, for all intents and purposes, probably has as little knowledge or awareness of these devices in the home, as they do of the safety devices in a vehicle.

Yet it's hard to imagine that courts would hold that a person has no 4th Amendment expectation of privacy in a device in their home, or that law enforcement could search such a device in their home without a warrant, merely because of the couple's lack of awareness. Indeed, the very genesis of the 4th amendment stems from colonists disgruntled with British invasions of their homes, and the very language of the 4th Amendment focuses on "t]he right of the people to be secure in their persons, **houses**, papers, and effects, against unreasonable searches and seizures . . . . (emphasis added)." Moreover, in 2001 the Supreme Court clarified that the 4th Amendment protects the privacy of homes, even when law enforcement doesn't physically enter, if their actions have the potential for invading that private sanctum. Specifically, in *Kyllo* v. U.S.,[97] the Supreme Court held that the use of a thermal imaging device by law enforcement, to monitor the radiation of heat coming from a home, while physically remaining outside of that home, is still considered a "search" of a 4th Amendment protected space, and thus required a search warrant.

And as the *Worsham Court* noted, the Supreme Court has previously recognized that a car's interior is also protected from unreasonable intrusions by the police under the 4th Amendment (although, concededly, the Supreme Court has also recognized that there is a reduced expectation of privacy in a vehicle, should there be probable cause to search a specific part of the automobile). [98]

In short, it seems like a dangerous road (pun intended) to consider the awareness of a specific, innocuous device (i.e., not inherently illegal, like drugs) installed in a private space – a home or vehicle - for purposes of assessing whether there's an REP in the data on the device, because it's the REP in the space itself that's key. And if there's an REP present in a private space, it should cover all devices within that space, both known and unknown.

The second question courts have wrestled with is whether the actions captured by these black-box devices are exposed to the public (i.e., in public view), thereby vitiating any argument that the actions are private and deserving of 4th amendment protection. Technically speaking, however, what is exposed to the

[97] 533 U.S. 27 (2001).
[98] Worsham, 227 So. 3d @ 604 (quoting New York v. Class, 475 U.S. 106, 114-115 (1986)); see also Carroll v. United States, 267 U.S. 132, 153 – 156 (1925).

public when a driver operates a vehicle is not his/her actions, but rather the results of the driver's actions, or "outward manifestations" as the *Mobley Court* of Appeals put it.[99] But the outward manifestations are not necessarily transparent as to the underlying actions causing these effects.

For example, a vehicle on a public roadway slowing down could be the result of the driver pressing the brake, removing his/her foot from the gas pedal, or even activating the parking brake (in extreme circumstances), each of which outwardly manifests in the same slowing of the vehicle. But the underlying cause is distinctly different inside the vehicle. Likewise, there can be a number of reasons that a vehicle appears to accelerate on a public roadway, in addition to the driver actually pushing the gas pedal. For example, the gas pedal could be trapped beneath the floor mat, or become "sticky" due to an inherent defect by the manufacturer.[100] While it may be a bit far-fetched today - since hacker's have only claimed to be able to hack into a vehicle's GPS tracking App and kill the car's engine- its not out of the realm of possibility that someday soon a vehicle's electronic system could be hacked and remotely manipulated to accelerate the vehicle.[101] Once again, the same outward manifestation, but caused by a variety of different actions inside the vehicle. Indeed, each of these actions may entail distinctly different legal culpability. A fatality caused by an inattentive driver accelerating into the rear of another vehicle may be handled vastly different from a case involving the same fatality, caused by the same accelerating vehicle, but with the precipitating factor being the manufacturer's "sticky" gas pedal defect.

In addition, there is a great deal of data collected by these devices that is not necessarily transparent to the public, such as "throttle position, engine revolutions, driver's seat belt status and brake switch status . . . and diagnostic information on the vehicle's systems."[102] And as these devices continue to evolve and collect increasingly more data – after all, we live in a data-driven economy – it may become harder to argue that the information collected was exposed to the public.

Finally, the third question courts have pondered when considering whether data captured by these devices is protected by the 4th Amendment relates to the type of information gathered; i.e., is it sensitive personal information, which the U.S. Supreme Court seems increasingly inclined to protect under the 4th

[99] See, 816 S.E.2d @ 774.
[100] Toyota to Pay $1.2B for Hiding Deadly 'Unintended Acceleration', Brian Ross, Joseph Rhee, Angela M. Hill, Megan Chuchmach and Aaron Katersky, ABC News, March 29, 2014, https://abcnews.go.com/Blotter/toyota-pay-12b-hiding-deadly-unintended-acceleration/story?id=22972214
[101] *Hacker Finds He Can Remotely Kill Car Engines After Breaking Into GPS Tracking Apps*, Lorenzo Franceschi-Bicchierai, Motherboard, Apr 24, 2019, https://www.vice.com/en_us/article/zmpx4x/hacker-monitor-cars-kill-engine-gps-tracking-apps.
[102] See, 816 S.E.2d @ 772.

Amendment. While the airbag device cases surveyed by these courts do not, as of yet, appear to contain the same level of sensitive, personal information as a cell phone or GPS, as these devices become smarter, with larger storage capacity, it's certainly foreseeable that the data they collect may eventually give rise to concerns similar to those considered by the *Jones* and *Riley* courts. As Georgia Court of Appeals Chief Judge Dillard observed in *Mobley*, the trajectory of technology seems to be toward greater, more precise data collection.[103] Likewise, the *Worsham* Court recognized that these devices tend to capture "more than what is voluntarily conveyed to the public . . . [j]ust as cell phones evolved to contain more and more personal information, as the electronic systems in cars have gotten more complex, the data recorders are able to record more information."[104] An example might help illustrate the concern.

Consider if these devices were to gather data about which seats are occupied while the vehicle is in motion, at what times, and the approximate weight of the people in those seats (assuming they don't already), presumably for the purpose of calculating the optimal speed and timing of airbag deployment. In such scenario, one could foresee this data becoming useful in other, non-crash-related contexts, such as in a divorce proceeding by a spouse attempting to prove infidelity on behalf of the other spouse, using evidence from the vehicle's device to prove the approximate size and weight of the person in the passenger seat, which coincidentally matches the size and weight of the person allegedly having an affair with the married spouse. Or consider a civil action by an employer, or car rental company, for violating employment rules/rental agreement that prohibits passengers in the vehicle at the time of operation.

Indeed, it's not hard to foresee a time when these devices begin recording voices, much like a plane's black box, in order to gain insight into what's happening in the vehicle compartment leading up to the crash. Did the driver attempt to avoid the crash, uttering words as he made that attempt? Or did the driver fail to even see/detect the issue until the very last moment, driving silently ignorant? Was the driver talking to himself, or another person, mumbling words and slurring speech, indicating the potential influence of alcohol or drugs? Regardless of the specific scenario, it would be hard to argue that the data captured in such cases does not rise to the level of personal and sensitive information.

In short, thinking through how this question may play out in the courts, given the amount of data currently collected, and the propensity for data collection to increase in the future, there is a good chance that courts will inevitably be left with no choice but to find a 4th Amendment protected REP in the data on these devices, thus requiring a search warrant for law enforcement to access this data. As the Georgia Court of Appeals Chief Judge

[103] 816 S.E.2d @ 776-777 (concurring opinion of Chief Judge Dillard).
[104] 227 So. 3d @ 606.

observed, "with technology of this nature rapidly developing, it is easy to imagine future cases presenting much thornier questions. For instance, had the ACM in this case included detailed GPS tracking information or other personal details of Mobley's everyday life, a warrantless search may have run afoul of the Fourth Amendment's protection of his reasonable expectation of privacy."[105]

Perhaps illustrative of the challenges that lie ahead, even before we come to final consensus on application of the 4th Amendment to airbag safety device data, we may face challenges in applying privacy laws to the data on these devices. Consider the California Consumer Privacy Act (CCPA), which went into effect in January 2020. Given the broad definition of "personal information" under the CCPA, which "arguably covers the majority of data that is collected by a vehicle," we may need to ask whether vehicle manufacturers and/or sellers need to comply with the CCPA when it comes to sales of vehicles to California residents, including the right to notice (lack of awareness of these devices being something both the Trial Court in *Diaz*, and the Florida Court of Appeals dissenting opinion in *Worsham* having highlighted), the right to opt-out (or in) to data collection by the device in the first place, not to mention the right to deletion of the data collected.[106] To borrow a phrase often used to refer to the Internet a decade ago, it appears that the "Information Superhighway" may be on a collision course with the real world highways upon which our vehicles drive today.

[105] 816 S.E.2d @ 776-777 (Dillard, Chief J., concurring).
[106] CCPA's potential impact in the automotive space, Eva Pulliam and Sarah Bruno, Oct 1, 2019, International Association of Privacy Professionals, https://iapp.org/news/a/ccpas-potential-impact-in-the-automotive-space/.