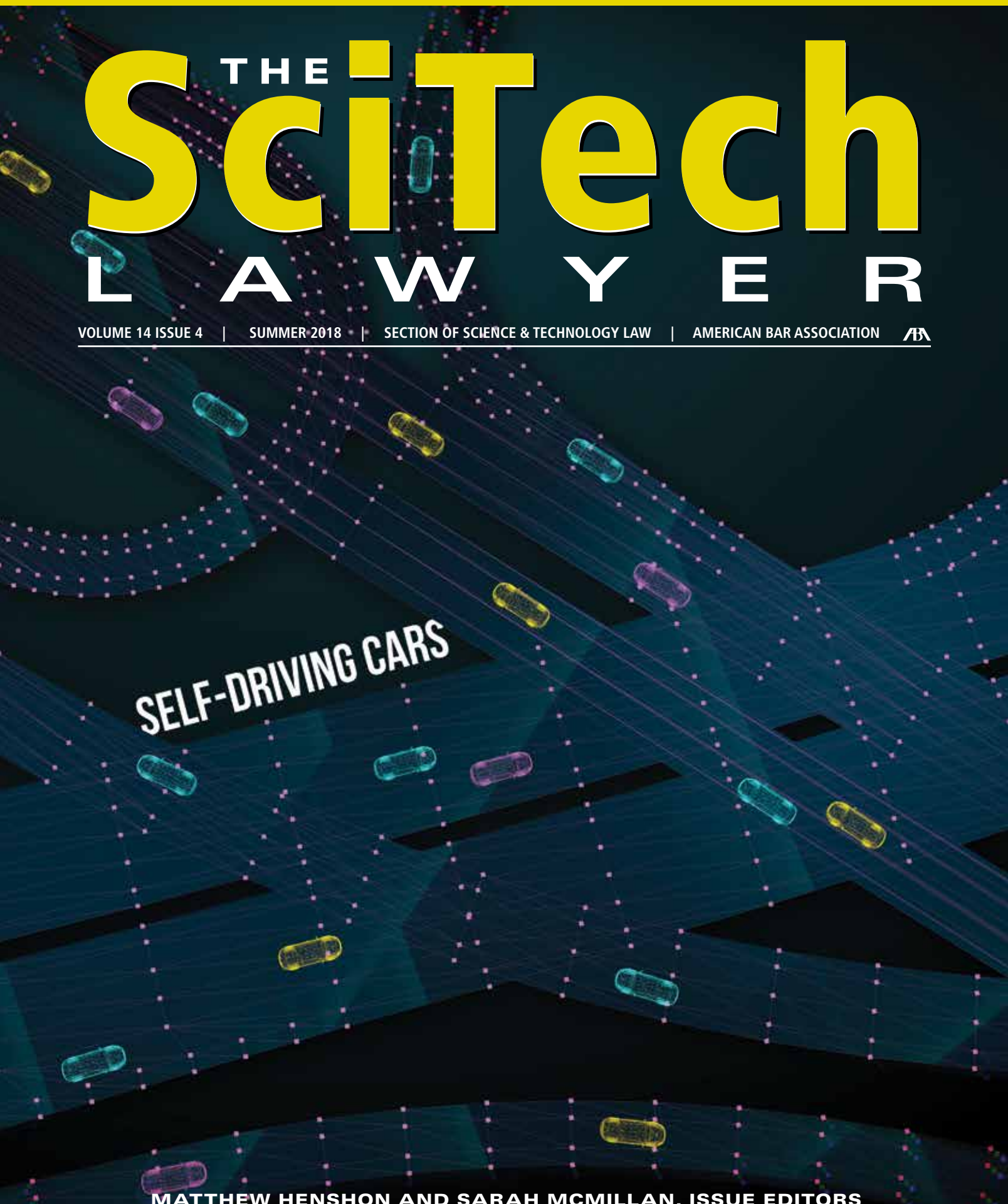
IN THIS ISSUE AUTONOMOUS VEHICLES • AV CYBERSECURITY • ROAD SAFETY

THE SciTech LAWYER

VOLUME 14 ISSUE 4 | SUMMER 2018 | SECTION OF SCIENCE & TECHNOLOGY LAW | AMERICAN BAR ASSOCIATION



MATTHEW HENSHON AND SARAH MCMILLAN, ISSUE EDITORS

THE SciTech LAWYER

The SciTech Lawyer (ISSN 1550-2090) is published quarterly as a service to its members by the Section of Science & Technology Law of the American Bar Association, 321 North Clark Street, Chicago, IL 60654-7598. It endeavors to provide information about current developments in law, science, medicine, and technology that is of professional interest to the members of the ABA Section of Science & Technology Law. Any member of the ABA may join the Section by paying its annual dues of $55. Subscriptions are available to nonmembers for $55 a year ($65 for foreign subscribers). Some back issues are available for $12 plus a $3.95 handling charge from the ABA Service Center, American Bar Association, 321 North Clark Street, Chicago, IL 60654-7598; 1-800-285-2221. Requests to reprint articles should be sent to ABA Copyrights & Contracts, www.americanbar.org/utility/reprint/Periodicals; all other correspondence and manuscripts should be sent to *The SciTech Lawyer* Contract Editor Melissa Vasich, melissa@vasich.com. For more information, visit www.americanbar.org/publications/scitech_lawyer_home.html. The material published in *The SciTech Lawyer* reflects the views of the authors and has not been approved by the Section of Science & Technology Law, the Editorial Board, the House of Delegates, or the Board of Governors of the ABA.

MESSAGE FROM THE CHAIR

David Z. Bodenheimer

SciTech Tackles the Latest Revolution: Autonomous Vehicles

The U.S. Department of Transportation described autonomous vehicles (AV) as "the greatest transportation revolution since the popularization of the personal automobile nearly a century ago." Like all revolutions, winners and losers will emerge. And like the earlier Model T revolution, the horse-and-buggy laws will lag the AV technology's dragster pace.

AV's Economic Drivers. With a $7 trillion global market looming, the AV revolution is financially inevitable. For the car data industry alone, McKinsey projects a $750 million global business by 2030. Efficiencies and savings include reducing 2.7 billion unproductive hours on American highways, saving $488 billion from injuries and deaths on the road, and boosting U.S. productivity by $448 billion.

AV's Winners and Losers. With fully automated roadways, up to 5 million truckers, taxi operators, and other drivers may be out of work. Some sectors and professions will contract (e.g., traffic police and auto repair), while others will surge (e.g., digital media, electronics, and freight transport). And perhaps billboards for traffic lawyers ("Had an accident? Call me") will vanish.

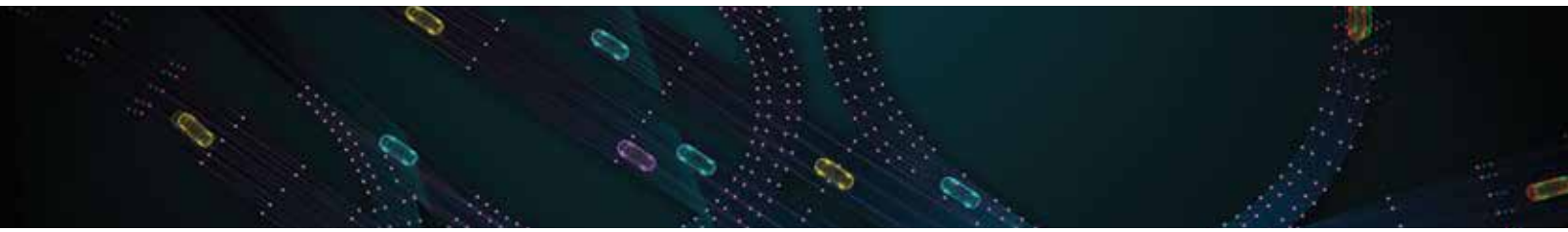
AV's Global Tire-Print. As world markets compete for the $7 trillion prize, the AV revolution is much broader than the auto manufacturers who already have heeded the AV green flag. The AV economics have attracted not only new manufacturers (e.g., Tesla and Rivian), but also passenger companies (e.g., Uber and Waymo), network leaders (e.g., AT&T and Ericsson), and other high-tech global names (e.g., Amazon, Microsoft, Hitachi, and Symantec). And this race to the AV checkered flag will take place not only on the streets, but also at sea and in the air with autonomous ships and aircraft, thus expanding the market and increasing the stakes.

SciTech's AV Leadership. In recent years, SciTech has showcased its expertise on AV issues. At the 2016 ABA Annual Meeting, Steve Wu led a panel on "Driverless Cars in the Fast Lane: Liability Ahead!" For the first IoT National Institute, Tim Goodman (Assistant Chief Counsel, National Highway Transportation Safety Administration) discussed federal efforts to promote AV safety and deployment, while the second IoT National Institute featured Cheri Falvey's mock trial illustrating risk allocation and emerging legal issues for the AV market. Similarly, SciTech presentations at the 2017 RSA conference included "Look Ma, no hands! Risk and liabilities in the era of Autonomous Cars" addressing AV and the law.

SciTech and the Future of AV Law. As today's edition of *The SciTech Lawyer* illustrates, AV technology is hitting the market well ahead of international and national laws, regulations, and standards originally designed for T-Models, Edsels, and muscle cars. In addition to the thought-provoking issues and AV expertise demonstrated in this edition, SciTech has the organization and leaders well suited to the heavy lifting needed to strike the critical balance between law, science, and technology on AV issues—including our committees tackling emerging IoT developments, privacy conundrums, insurance technology puzzles, information security risks, and more.

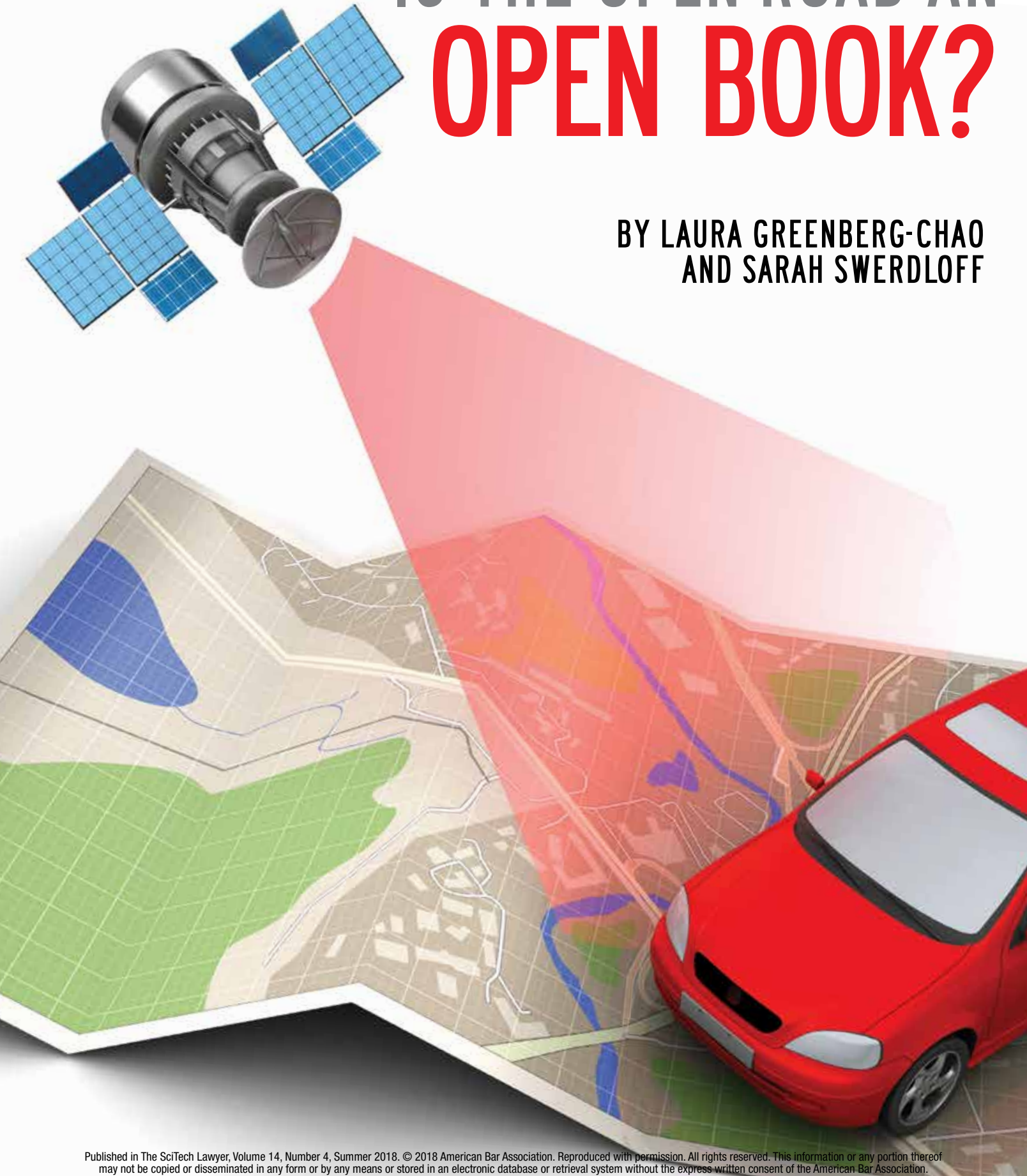
While the vehicles may be on autopilot, the law should not be. SciTech must seize this opportunity to bring its unique and deep expertise to shaping the law during this AV revolution. ◆

TABLE OF CONTENTS



IS THE OPEN ROAD AN OPEN BOOK?

BY LAURA GREENBERG-CHAO
AND SARAH SWERDLOFF



Remember when you could get in your car, head out on the open road, and to the rest of the world, your whereabouts were a mystery? You used a map to figure out where to go. You used a pay phone at a rest stop or a landline at your destination to call home. Your car neither created nor stored any data—it was just a vehicle to get you from point A to point B. And if someone wanted to know where you were or what you were doing, they had to get into their vehicle and follow you.

But think about how far we have come. When you own a driverless car, which you might in your lifetime, it will not just be a vehicle. Even more so than your cell phone, it will be both the source of and the storage for tremendous amounts of data: information about where you are, where you've been, what you've been doing, what you are planning to do—data that show your habits, like how you take the same route every second Tuesday when you go to an out-of-the-way park to meet someone, and your character, like how you turn off the cameras in your car each time you go to that park. And now, if someone, and in particular, the police, want to know even the littlest detail about you, those data are right there in your driverless car.

So the question for driverless cars is, how and when should the police be able to access your data? Or, put another way, should your open road be law enforcement's open book?

Data in Driverless Cars

Privately owned driverless cars will collect and house a treasure trove of information. With the hope that driverless cars will reduce car accidents (or even make them obsolete), data collected in those cars go far beyond their early predecessors, black boxes in airplanes, which recorded information related to operation and functioning. In addition to GPS data related to the most recent trip taken, autonomous cars will retain historical data as well—where the driver has been, how frequently he goes there, all of the stops he makes along the way, and places that he has stopped visiting.[1] As illustrated by the horrific images from just before an Uber self-driving car struck a pedestrian in Arizona, video and photographic cameras and sensors will capture not only what is going on inside the car, but also what is happening outside.[2] "Many new vehicle models already connect some of these dots, using previously captured data to infer a driver's preferences, and suggest certain songs or routes to them . . . [and] at their most extreme, cars will even be able to know *who* is behind the wheel."[3]

There has not yet been comprehensive legislative action related to autonomous vehicles on the state or federal level, but the piecemeal statutes governing accident-related data in cars focus on the privacy of such data.[4] In 2015, Congress passed the Driver Privacy Act, which declared that information collected by event data recorders (EDRs), such as how fast a car was travelling before a crash and whether the brakes were applied, belonged to the owner of the vehicle.[5] In a similar vein, the seventeen state statutes that set forth rules regarding EDRs generally consider the data in a vehicle to be private.[6]

No Data Access for Law Enforcement . . .

At one extreme, there are those who believe that this tremendous amount of data should be *so* private that individuals should be able to lock out anyone, even law enforcement with a lawful search warrant based on probable cause.[7] We need only look to the parallel context of data in cell phones to see how this has played out when data are password protected. Courts have generally refused to force a suspect to reveal his password based on the Fifth Amendment's prohibition against self-incrimination. In *United States v. Kirschner*, for example, the government sought a court order to force the defendant to reveal his computer password.[8] The court rejected the government's request, citing an oft-used analogy that a defendant could be compelled to reveal "a key to a strongbox containing incriminating documents," but he could not be compelled to reveal "the combination to his wall safe."[9]

The bottom line is that where data in vehicles are encrypted by a password, law enforcement is going to face an uphill battle in accessing it, even with a valid search warrant and for a legitimate and lawful purpose.

. . . Easy Data Access for Law Enforcement

At the opposite extreme from the password-protected data that provide virtually no access to law enforcement is the third-party doctrine. Until recently, data held by a third-party (such as banks, Internet service providers, email servers, and cell phone companies) were available to law enforcement under a lower standard than the probable cause required for a search warrant. That is, because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," the Fourth Amendment does not protect such data in the hands of third parties.[10]

Instead, these data are accessible by various methods that are significantly less onerous for law enforcement to satisfy than the standard required for a search warrant (probable cause). Law enforcement can issue an administrative or grand jury subpoena, without court authorization, for certain types of data (such as basic phone subscriber information) as long as the information sought satisfies the low bar of being "relevant to a criminal investigation."[11] Other types of data (such as phone records showing how long a call was, whether a communication was a text or a call, or the method of payment used

for an account) are governed by the federal Stored Communications Act (SCA), which requires a level of suspicion somewhere between the subpoena standard and probable cause.[12]

In its traditional form, the third-party doctrine would have provided various methods of accessing data in driverless cars where law enforcement either does not have the car itself or does not have enough information for a search warrant, or where the data are password protected. But this doctrine seems to be headed for a significant legal restructuring.

Access to Data in Driverless Cars: A Compromise

Recent legal and technological trends seem to be cruising towards some compromises between privacy and law enforcement interests. The treasure trove of data in driverless cars, then, is likely to be neither easily accessible nor absolutely inaccessible to legitimate law enforcement investigations. If the recent oral arguments in *Carpenter v. United States* are any indication, the "backdoor" that has been open to law enforcement through the third-party doctrine is about to be at least partially closed, benefitting privacy rights. On the other end of the spectrum, the roadblocks created by passwords are giving way to biometric encryption, whereby encryption is dependent on a unique biological identifier such as a fingerprint, voice, eye, or face, which ensures data security but also can benefit law enforcement access, as it is unfettered by the Fifth Amendment.

Third-Party Doctrine Changes

Rapidly changing technology has forced the court to acknowledge that the third-party doctrine does not fit the world of today and tomorrow. In 2012, in the course of finding that attaching a GPS device to a car was a Fourth Amendment search (thus requiring a warrant), Justice Sotomayor noted that the third-party doctrine may be "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[13]

More recently, in the fall of 2017, the justices' questions in the argument over *Carpenter v. United States* again suggested weakening of the third-party doctrine.[14] The FBI had relied on the SCA to obtain cell site location information from Carpenter's cell phone provider, thus enabling the government to track his location for 127 days.[15] Carpenter challenged the government's retrieval of the data, arguing that because the data were subject to the Fourth Amendment, the FBI had needed a search warrant based on probable cause rather than the lower standard court order under the SCA.[16]

Although the deputy solicitor general harkened back to *Smith* to argue that Carpenter had voluntarily given his information to third parties for storage, the justices seemed uncomfortable with the notion of "voluntariness" in this context and were more inclined to recognize Fourth Amendment privacy rights requiring a probable cause to search. [17] Justice Sotomayor highlighted the absurdity of the government being "able to [conduct the tracking] without probable cause and a warrant" simply because the information is sent from the device back to a third party.[18] Justice Breyer went as far as to wonder out loud whether there should be an exception to the third-party doctrine due to the rapid advances in technology, especially since there is now the ability to surveil an individual for an extremely long period of time.[19]

Given this level of skepticism, it seems unlikely that the Court will uncategorically bless law enforcement's continued reliance on the lower standard of the SCA to obtain data from third parties. What is more likely is that by the time driverless cars become commonplace, law enforcement will have to present third parties with a search warrant based on probable cause in order to obtain at least some of the car's data.

Biometric Encryption Yields to Access

Driverless cars may also reconcile privacy interests and law enforcement interests in the context of data security. Rather than relying on password security, current models of driverless cars employ fingerprint recognition, eye scans, voice recognition, or facial recognition for data security and to operate the vehicle.

As compared to password security, which can make law enforcement access impossible under the Fifth Amendment, biometric encryption is subject to a very different legal analysis. Whereas passwords have been considered testimonial, compelling an individual to provide his fingerprint to unlock a biometric encryption "elicit[s] only physical evidence . . . and [does] not reveal the contents of his mind."[20] In other words, because biometric encryption falls outside the protections of the Fifth Amendment, law enforcement could force a suspect to unlock data using biometrics.[21]

Conclusion

Driverless cars will not be an open book for law enforcement. But between a new version of the third-party doctrine and the legal analysis around biometric encryption, privacy interests and legitimate law enforcement interests may end up sharing the road. ◆

Laura Greenberg-Chao *(lgreenbergchao@henshon.com) is a partner at Henshon Klein LLP in Boston, Massachusetts. As a litigator, she represents clients in a wide variety of technology fields.* ***Sarah Swerdloff*** *(sswerdloff@henshon.com) is a transactional associate at Henshon Klein LLP.*

Endnotes

1. Bridget Clerkin, *Autonomous Cars, Big Data, and the Post-Privacy World*, DMV.ORG (Oct. 2, 2017), https://www.dmv.org/articles/self-driving-vehicles-privacy-concerns.

2. *Police Release Dash Cam Video of Deadly Arizona Crash Involving Uber SUV*, CBS LOCAL N.Y. (Mar. 21, 2018), http://newyork.cbslocal.com/2018/03/21/uber-suv-self-driving-crash-video.

3. *Id.*

4. Although manufacturers of autonomous vehicles hope that accident reconstruction data will be unnecessary in driverless cars, the

National Highway Traffic Safety Administration (NHTSA) has mandated that all cars manufactured after September 2014 include an event data recorder. Kristen Hall-Geisler, *The Importance of Black Boxes in an Autonomous Automotive Future*, TechCrunch (May 13, 2016), https://beta.techcrunch.com/2016/05/13/the-importance-of-black-boxes-in-an-autonomous-automotive-future/. The NHTSA also is making proposals specifically related to autonomous vehicles: In 2016, they proposed mandatory privacy measures for communications between self-driving vehicles about speed, location, and passengers in each vehicle. Press Release, NHTSA, U.S. DOT Advanced Deployment of Connected Vehicle Technology to Prevent Hundreds of Thousands of Crashes (Sept. 12, 2017), https://www.nhtsa.gov/press-releases/us-dot-releases-new-automated-driving-systems-guidance. They also held a workshop in 2017 for stakeholders to discuss issues including privacy for self-driving cars. Fed. Trade Comm'n, Connected Vehicles: Privacy, Security Issues Related to Connected, Automated Vehicles (June 28, 2017), https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.

5. Driver Privacy Act of 2015, S. 766, 114th Cong. § 24302.

6. Those states include Arkansas, California, Colorado, Connecticut, Delaware, Maine, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Oregon, Texas, Utah, Virginia, and Washington. *Privacy of Data from Event Data Recorders: State Statutes*, Nat'l Conference of State Legislatures (Jan. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx. For example, New York requires manufacturers to disclose the presence of EDRs in the owner's manual and prohibits the retrieval of EDR data without the owner's consent or a court order unless the retrieval is for safety research, mechanical diagnosis, or dispatching emergency medical personnel. N.Y. Veh. & Traf. Law § 416-b (2012).

7. *See, e.g.*,Matt Apuzzo, *Should the Authorities Be Able to Access Your iPhone?*, N.Y. Times (Feb. 17, 2016).

8. 823 F. Supp. 2d 665 (E.D. Mich. 2010).

9. *Id.* at 668 (quoting Doe v. United States, 487 U.S. 201, 219 (1987) (Stevens, J. dissenting)). *See*, *e.g.*, United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335 (11th Cir. 2012) (holding that a person accused of possessing child pornography may assert his Fifth Amendment privilege to avoid decrypting a hard drive because decryption and production were testimonial); Commonwealth v. Baust, 89 Va. Cir. 267 (Cir. Ct. 2014) (holding that compelling strangulation defendant to produce password to encrypted cell phone would violate the Fifth Amendment). But not all courts come out the same way. A Massachusetts court found that because the ownership of a cell phone was a "foregone conclusion" (that is, there was sufficient proof that the defendant owned the phone independent of his knowledge of the password), compelling him to produce the password did not violate the Fifth Amendment. *In re* a Grand Jury Investigation, 92 Mass. App. Ct. 531 (2017).

10. Smith v. Maryland, 442 U.S. 735 (1979).

11. 18 U.S.C. § 2703(c)(2) (2009). *See*, *e.g.*, 21 U.S.C.A. § 876(a) (1988) (authorizing attorney general to issue subpoenas in connection with drug investigations).

12. 18 U.S.C. § 2703(c) (2009). For a search warrant, there must be a "fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 214 (1983). Under the SCA, a third party must disclose certain telecommunications records when "specific and articulable facts show that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation". 18 U.S.C. § 2703(d) (2012), https://www.law.cornell.edu/supct/cert/16-402.

13. U.S. v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring). For an interesting discussion of how *Jones* affects privacy rights for driverless cars, see Matt Henshon, *Where Does Privacy Go from Here?*, 30 Unmanned Sys., no. 9, Sept. 2012.

14. *Carpenter v. United States*, Oyez (Apr. 3, 2018), https://www.oyez.org/cases/2017/16-402.

15. Jeffrey Rosen, *A Liberal-Conservative Alliance on the Supreme Court Against Digital Surveillance,* The Atl. (Nov. 30, 2017), https://www.theatlantic.com/politics/archive/2017/11/bipartisanship-supreme-court/547124/.

16. Madelaine Horn & Conley Wouters, *LII Supreme Court Bulletin: Carpenter v. United States*, Legal Info. Inst., https://www.law.cornell.edu/supct/cert/16-402.

17. Rosen, *supra* note 15.

18. Oral Argument of Sotomayor at 45:42, Carpenter v. United States, Oyez, https://www.oyez.org/cases/2017/16-402. Justice Sotomayor declared outright:

> the government cannot intrude on those [constitutional] privacy interests without a warrant. We're not saying they can't ever. They've just got to have articulable facts based on reliable information, sworn to in an affidavit, that can provide probable cause to believe that this individual is involved in criminal activity.

19. Amy Howe, *Argument Analysis: Drawing a Line on Privacy for Cellphone Records, but Where?*, SCOTUSBlog (Nov. 29, 2017, 2:43 PM), http://www.scotusblog.com/2017/11/argument-analysis-drawing-line-privacy-cellphone-records.

20. State v. Diamond, 905 N.W.2d 870, 872 (Minn. Ct. App. 2018). *See also Matter of Search Warrant Application for [redacted text],* No. 17M85, 2017 WL 456861, at *4 (N.D. Ill. Sept. 18, 2018) (holding that compelled act of placing finger on device was not an act of communication and therefore not testimonial); Commonwealth v. Baust, 89 Va. Cir. 267, 268 (2014) (holding that defendant could be compelled to provide fingerprint in order to unlock phone).

21. Not all courts agree with this analysis. A federal magistrate judge rejected a provision in a search warrant compelling any individual present at location of the search to provide a fingerprint to unlock such devices. In re Application for a Search Warrant, 236 F. Supp. 3d 1066 (N.D. Ill. 2017). In addition to finding that the request was overbroad and not supported by enough particularity, the court suggested that obtaining fingerprints *would* violate the Fifth Amendment. *Id.* at 1070, 1074.