No. 16-15496

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

HELENE CAHEN, et al.,

Plaintiffs-Appellants,

v.

TOYOTA MOTOR CORPORATION, et al.,

Defendants-Appellees.

On Appeal from the United States District Court
for the Northern District of California, San Francisco, Case No. 15-01104
The Honorable William Horsley Orrick III, District Judge

Brief of Amicus Curiae Electronic Privacy Information Center in Support of Plaintiffs-Appellants and in Support of Reversal

---

Marc Rotenberg
Alan Butler
Aimee Thomson
Electronic Privacy Information Center
1718 Connecticut Ave. N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for Amicus Curiae

August 5, 2016

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(c), Amicus Curiae Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE AMICUS[1]

The Electronic Privacy Information Center ("EPIC")[2] is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

For more than a decade, EPIC has been concerned about the growing risks to public safety resulting from the increasing collection and use of personal data concerning the operation of motor vehicles. *See* EPIC, Comments, Docket No. NHTSA-2002-13546 (Feb. 28, 2003)[3] ("There need to be clear guidelines for how the data can be accessed and processed by third parties following the use limitation and openness or transparency principles."). EPIC has written extensively on the safety and privacy implications of the connected devices in general, and connected cars in particular.[4] In November 2015, EPIC testified before Congress on the risks

---

[1] The parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief. Counsel for a party did not author this brief, in whole or in part.

[2] EPIC IPIOP clerks Natasha Amlani, Lindsey Barrett, Ellie Moscardini, Filippo Raso, Uri Sabach, and Janet Zhang assisted with the preparation of this brief.

[3] https://epic.org/privacy/drivers/edr_comments.pdf.

[4] *E.g.*, Marc Rotenberg, *Steer Clear of Cars that Spy*, USA Today (Aug. 18, 2011), http://usatoday30.usatoday.com/news/opinion/editorials/2011-08-18-car-insurance-monitors-driving-snapshot_n.htm; Marc Rotenberg, *Are Vehicle Black Boxes A Good Idea?*, at 21, Costco Connect (Apr. 2013); EPIC, *Automobile Event Data*

posed by connected cars and urged it to establish privacy and cybersecurity rules that protect driver data and prohibit malicious hacking. *The Internet of Cars: Hearing Before the H. Subcomm. on Info. Tech and the H. Subcomm. on Transp. and Pub. Assets of the H. Comm. on Oversight and Gov't Reform*, 114th Cong. (2015) (statement of Khaliah Barnes, EPIC Associate Director and Administrative Law Counsel).[5] EPIC has also submitted comments on the privacy and cybersecurity implications of connected cars to the National Telecommunications and Information Administration, the Federal Trade Commission, and the National Highway Traffic Safety Administration. *E.g.*, EPIC, Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, Docket No. 160331306-6306-01 (June 2, 2016);[6] EPIC, Comments on Federal Motor Vehicle Safety Standards: "Vehicle-to-Vehicle (V2V) Communications," Docket No. NHTSA-2014-0022 (Oct. 20, 2014);[7] EPIC, Comments on the Privacy and Security Implications of the Internet of Things (June 1, 2013);[8] EPIC et al., Comments on the Federal Motor Safety Standards; Event

---

Recorders (Black Boxes) and Privacy (2016), https://epic.org/privacy/edrs/; EPIC, *Internet of Things* (2016), https://epic.org/privacy/internet/iot/.

[5] https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf.

[6] https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf.

[7] https://epic.org/privacy/edrs/EPIC-NHTSA-V2V-Cmts.pdf.

[8] https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.

Data Recorders, Docket No. NHTSA-2012-0177 (Feb. 11, 2013);[9] EPIC, Comments, Docket No. NHTSA-2004-18029 (Aug. 13, 2004).[10]

Courts routinely look to EPIC for insight about emerging privacy and civil liberties issues. In the field of consumer protection and federal jurisdiction, EPIC has authored several substantial briefs as amicus curiae. *E.g.*, *Spokeo v. Robins*, 578 U.S. ___, 136 S. Ct. 1540 (2016) (arguing that the violation of a consumer's privacy rights under the Fair Credit Reporting Act constitutes an injury-in-fact sufficient to confer Article III standing); *Clapper v. Amnesty Int'l. USA*, 568 U.S. ___, 133 S. Ct. 1138 (2013) (arguing that journalists, attorneys, and others who communicated with individuals abroad faced a reasonable fear that their communications would be subject to government surveillance); *First American Fin. Corp. v. Edwards*, 567 U.S. ___, 132 S. Ct. 2536 (2012) (*per curiam*) (arguing that consumers can have standing to sue based on violations of their rights established under federal law); *Perry v. CNN*, No. 16-13031 (11th Cir. filed July 22, 2016) (arguing that smartphone device identifiers are personally identifiable information under the Video Privacy Protection Act, and that the Act covers users of mobile video apps); *Alleruzzo, et al., v. SuperValu, Inc., et al.*, Nos. 16-2378 & 16-2528 (8th Cir. filed July 19, 2016) (arguing that data breach victims have

[9] https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf.
[10] https://epic.org/privacy/drivers/edr_comm81304.html.

standing to sue based on companies' inadequate data security practices); *In re Nickelodeon Consumer Privacy Litigation*, No. 15-1441, 2016 WL 3513782 (3d Cir. June 27, 2016) (addressing the definition of personally identifiable information under the VPPA, as applied to Internet addresses and other unique persistent identifiers); *Storm v. Paytime, Inc.*, No. 15-3690 (3rd Cir. filed Apr. 18, 2016) (arguing that data breach victims have standing to sue based on exposure of their Social Security Numbers and other sensitive personal information).

SUMMARY OF THE ARGUMENT

"Connected vehicles" expose American drivers to the risks of data breach, auto theft, and physical injury. The internal computer systems for these vehicles are subject to hacking, unbounded data collection, and broad-scale cyber attack. Despite this extraordinary risk, car manufacturers are expanding the reach of networked vehicles that enable third party access to driver data and vehicle operational systems. The plaintiffs in this case seek the opportunity to present legal claims stemming from the defendants' sale of vehicles that place them at risk. They should be allowed to proceed.

The lower court misapplied the relevant caselaw when it dismissed the plaintiffs' claims for lack of Article III standing. The court failed to examine whether the plaintiffs had suffered *violations of law*. Instead, the lower court focused on whether consequential harms were "certainly impending," thereby conflating legal injury with harm. The court also underestimated the substantial risk to public safety of connected cars and misconstrued the plaintiffs' invasion of privacy claim. Whether or not the court ultimately agrees with the allegations presented, they are clearly sufficient to establish Article III standing.

ARGUMENT

I. Article III standing turns on whether the plaintiffs have suffered a legal injury, not on whether they will suffer consequential harm.

"Injury is the illegal invasion of a legal right; damage is the loss, hurt, or harm that results from the injury." 22 Am. Jur. 2d *Damages* § 2 (2016). Despite this clear and important distinction, the lower court conflated injury-in-fact, i.e. the illegal invasion of a legal right, and consequential harm in the analysis of standing. Several other courts, and even plaintiffs' attorneys, have made this same mistake. The confusion arises from a semantic trick,[11] proffered by defendants in cases on standing, that seeks to avoid consideration of valid claims on the merits. The confusion between legal injury and consequential harm led the lower court in this case to apply a "certainly impending consequential harm" test that has no basis in Article III or the U.S. Supreme Court's jurisprudence. The Supreme Court's decision in *Clapper* concerned a fundamentally different type of claim—an injunction to prevent future violations of law—that bears no relation to claims brought in this and other data security cases. This Court should vacate and remand for a proper analysis of the standing issue based on the legal injuries alleged by the plaintiffs.

[11] In common English, the terms "injury" and "harm" are considered synonyms. Webster's Pocket Thesaurus of the English Language 134 (2001). However, in law the terms are clearly distinguishable. An injury is the "violation of another's legal

A. Article III requires a court to analyze whether plaintiffs have alleged sufficient *violations of law*.

To invoke Article III standing, a plaintiff must (1) suffer an injury-in-fact that is (2) fairly traceable to the defendant and (3) is likely to be redressed by a favorable judicial decision. *Spokeo v. Robins*, 578 U.S. ___, 136 S. Ct. 1540, 1547 (2016); *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992). Courts must find standing for each alleged claim. *Int'l Primate Prot. League v. Adm'rs of Tulane Educ. Fund*, 500 U.S. 72, 77 (1991), *superseded by statute on other grounds*, Federal Courts Improvement Act of 1996, Pub. L. No. 104-317, 110 Stat. 3847.

Injury-in-fact requires the plaintiff to suffer an "invasion of a legally protected interest,"—a *legal injury*—that is (1) "concrete and particularized" and (2) "actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560. Legal injury is distinct from the "disadvantage that may flow from" the injury. *Warth v. Seldin*, 422 U.S. 490, 503 n.13 (1975); *see, e.g.*, *In re Google Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 134 (3d Cir. 2014); *Spokeo*, 136 S. Ct. at 1552 (Thomas, J. concurring).

Functionally, there are three parts to the injury-in-fact test. First, the invasion of the legal interest must be concrete. A "concrete" invasion is "*de facto*," meaning it must "actually exist," but may be "intangible." *Spokeo*, 136 S. Ct. at

---

right, for which the law provides a remedy." *Injury*, Black's Law Dictionary (10th ed. 2014). Harm, by contrast, is "material or tangible detriment." *Harm*, *id.*

1548–49. Both "history and the judgment of Congress" are instructive when deciding if an intangible legal injury is "concrete." *Id.* at 1549. Concrete, intangible, legal injuries sometimes have "a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* (referring to legal injury when using "harm"). But Congress has the authority to elevate "concrete, *de facto* injuries that were previously inadequate at law" to the "status of legally cognizable injuries." *Id.* (internal quotation marks omitted). As Justice Kennedy explained in *Lujan*, "Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before . . . ." *Lujan*, 504 U.S. at 580 (Kennedy, J, concurring). Justice Kennedy further explained that "[a]s Government programs and policies become more complex and far reaching, we must be sensitive to the articulation of new rights of action that do not have clear analogs in our common-law tradition." *Id.*

Most rights established by Congress are substantive, and their violation is therefore concrete. But the Supreme Court made clear that even procedural violations can give rise to standing. *Spokeo*, 136 S. Ct. at 1549. Only a "bare procedural violation" that is "divorced from any concrete harm" fails to confer standing. *Id.* (referring to damages when using the term "harm"). Thus, following

Spokeo and *Lujan*, consequential harm is only relevant to the standing inquiry where a plaintiff has alleged a "bare" procedural violation of law.

Second, the invasion of the legal interest must be particularized. A "particular" invasion must "affect the plaintiff in a personal and individual way," where the plaintiff is "among the injured." *Lujan*, 504 U.S. at 560 n.1, 563 (internal quotation marks omitted). Simply put, if the violated right belongs to the plaintiff, the invasion is particularized.

Finally, the invasion of the legal interest must be actual or imminent. That is, the defendant must have already violated or will imminently violate the plaintiff's legal right. An "actual" legal injury must have already occurred, while an "imminent" legal injury must be "*certainly* impending." *Clapper v. Amnesty Int'l, USA*, 568 U.S. ___, 133 S. Ct. 1138, 1147 (2013) (emphasis in original) (internal quotation marks omitted). Several courts—including the lower court here—misunderstand *Clapper* to require that plaintiffs allege that *consequential harms* have already occurred or are "certainly impending." *E.g.*, Order on Mot. Dismiss 15, ECF No. 82 [hereinafter Order]; *Duqum v. Scottrade, Inc.*, No. 15-1537, 2016 WL 3683001 (E.D. Mo. July 12, 2016). But *Clapper* concerned injunctive relief to prevent future violations of law. *Clapper*, 133 S. Ct. at 1155. *Clapper* is entirely irrelevant to "actual" (not "imminent") injury claims such as here, where the plaintiffs allege that the defendants already violated California law. First Am.

Compl. 16–26, ECF No. 37. Contrary to the lower court's assertion, nowhere does *Clapper* create, or Article III mandate, a "certainly impending consequential harm" standard.

B. The lower court failed to analyze whether the plaintiffs' alleged legal injuries were actual, concrete, and particularized.

The plaintiffs in this case alleged violations of five statutory rights, violations of two common law rights, and violation of a California constitutional right. Order 4. A proper standing analysis requires the court to determine whether each of the plaintiffs' alleged violations *of their legal rights* is concrete, particularized, actual or imminent, whether the violation was caused by the defendant, and whether the violation is redressable by the court. But the lower court failed entirely to conduct this analysis. Instead the court incorrectly considered the probability of *consequential harms* to the plaintiffs stemming from the alleged vehicle vulnerabilities: risk of hacking, economic loss, and risk of identity theft. *Id.* 12–23. This Court should vacate and remand for a proper analysis of the standing issue based on the legal injuries alleged by the plaintiffs.

II. Drivers face security risks due to the vulnerability of connected cars.

The lower court dismissed the plaintiffs' claims in part because it found that they did not "face a credible risk of hacking." Order 17. Although standing turns on whether the plaintiffs alleged sufficient *legal* injury, see Part I, *supra*, the lower

court's conclusion is also wrong because it fundamentally misunderstands the security vulnerabilities created by connected cars.

A. Connected cars are inherently vulnerable because they rely on an interconnected system without authentication or encryption.

Cars today are dependent on extraordinarily complex onboard computer systems. According to the Government Accountability Office, the typical modern high-end car contains over 100 million lines of code—substantially more than a Boeing 787 passenger airline, which contains 6.5 million lines of code, or an F-22 U.S. Air Force jet fighter, which contains 1.7 million lines. U.S. Gov't Accountability Office, GAO-16-350, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack* 8–9 (Mar. 2016)[12] [hereinafter GAO Report]. As these vehicles have become more complex, the potential for software errors and related vulnerabilities correspondingly rise. *Id*; *see generally* Craig Smith, *The Car Hacker's Handbook: A Guide for the Penetration Tester* (2016). But car manufacturers have failed to take adequate steps to address these vulnerabilities.

Cars were first equipped with computer-controlled components in the late 1970s to automate basic engine functions, improve engine performance and fuel efficiency, and lower vehicle emissions. GAO Report, *supra*, at 6–7; Roderick

[12] http://www.gao.gov/assets/680/676064.pdf.

Currie, *Developments in Car Hacking*, Sans Inst. InfoSec Reading Room 2 (2015).[13] Since then, these Electronic Control Units ("ECUs") have grown in complexity, replacing or controlling many mechanical functions. GAO Report, *supra*, at 6–7. The typical modern vehicle now relies on computerization for almost everything from "engine management to steering, braking, climate control, navigation, [and] infotainment." Currie*, supra*, at 3; *see* Ben Wojdyla, *How It Works: The Computer Inside Your Car*, Popular Mechs. (Feb. 21, 2012).[14]

To reduce bulky wiring and point-to-point connections between ECUs, automakers began to locate ECUs on a centralized network bus, the Controller Area Network bus ("CAN bus"). GAO Report, *supra*, at 7; *see generally* Wilfried Voss, *A Comprehensible Guide to Controller Area Network* 10–14 (2005). Developed in the 1980s, the CAN bus is "the most commonly used in-vehicle communication network or bus." GAO Report, *supra*, at 7. Analogous to a freeway system, the CAN bus handles the communications from the majority of a vehicle's computerized components, each of which connect to the central bus via electronic "on and off ramps." Wojdyla, *supra*. As a result, the vehicle's engine management system, brake controller, airbags, seatbelt pretensioners, door locks, gauge cluster,

[13] https://www.sans.org/reading-room/whitepapers/internet/developments-car-hacking-36607.
[14] http://www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/.

sound system, seat controls, communications systems, and telematics units are all interconnected. Currie, *supra*, at 4–5.

While the CAN bus has been an efficient way to link operational components, it leaves cars inherently vulnerable to malfunction and attack. *Id.* at 9. Because all sections of a vehicle's CAN bus connect back to each ECU, the "window switches have a potential path of communication to the brake controller, the entertainment system has a channel to communicate through to the vehicle's airbags, and so on." *Id.* at 10. An attacker can enter through a vulnerability in the infotainment system, for example, and then pivot to exploit the vehicle's safety or control systems.

Had CAN bus technology been designed with security in mind, entertainment and convenience system components would not be able to communicate directly with critical vehicle control systems. *Id.* at 9. Network segmentation, for example, prevents hackers from exploiting a "trivial vulnerability in a non-sensitive system" to gain access to critical components within the network. *Id.* at 10; *see* Ctr. for Internet Sec., *The CIS Critical Security Controls for Effective Cyber Defense, Version 6.0* 42 (2015) ("[O]nce inside a network, many intruders attempt to target the most sensitive machines."). But the CAN bus architecture fails to implement this "fundamental part of secure system design." Currie, *supra*, at 10. While some limited communication will likely need

to occur between safety-critical and non-safety-critical systems, experts agree that domain separation is a very effective mitigation strategy. GAO Report, *supra*, at 22. Aftermarket firewall systems can also be added to existing cars to limit the free flow of information on the CAN bus. *Id.* at 23–24.

The CAN bus also lacks device authentication, allowing anyone with access to the system, authorized or not, to control vehicle components. Currie*, supra*, at 10–11. Data such as cabin temperature, steering input, and vehicle speed are constantly accessible by every component connected to the CAN bus, whether or not the component requires that information. *Id.* at 7. If a third party gains access to the CAN bus, she can mimic the CAN protocol and send malicious data messages that "will then be picked up and processed by listening controllers." *Id.* at 11. This is especially problematic because vulnerable wireless systems such as Bluetooth or GPS systems can provide access to the CAN bus. GAO Report, *supra*, at 14. This means that vulnerabilities in the car's wireless systems, the new "connected car" features, have exposed drivers to the threat of remote control by malicious attackers.

This problem is compounded because the CAN bus is natively unencrypted. Junko Yoshida, *CAN Bus Can Be Encrypted, Says Trillium*, EE Times (Oct. 22,

2015).[15] Because the CAN data is unencrypted, anyone with access to the CAN bus will be able to review and mimic the CAN messaging language. Currie, *supra*, at 13. The lack of encryption also enables malicious actors to modify or create CAN messages. *Id.* "Without some form of encryption, there is no way to guarantee message integrity or authenticity." *Id.* CAN manipulation is "trivial in its level of difficulty," *id.* at 11, and third-party products enable even a novice user to listen to traffic on the CAN bus with physical access to the vehicle. *See, e.g.*, CANdo, *CAN Bus Analyser* (2015).[16]

Worst of all, most of the technological fixes needed to secure connected cars "cannot be added on existing vehicles; rather, they must be incorporated into the vehicle design and production process," which takes "approximately 5 years to complete." GAO Report, *supra*, at 23. As a result, newly released models include security protections based on five-year-old threats, *id.* at 28—a lifetime in the computing world. The one exception is "intrusion detection and prevention systems," some of which "can be incorporated onto existing vehicles." *Id.* at 24.[17] As a result of modern automobile design, millions of cars on the road are vulnerable and pose a serious security risk to their occupants and to others.

[15] http://www.eetimes.com/document.asp?doc_id=1328081.
[16] http://www.cananalyser.co.uk.
[17] Message authentication and encryption, however, "cannot be easily incorporated onto CAN buses, as CAN does not provide sufficient bandwidth to host these protections." GAO Report, *supra*, at 25.

B. The lower court incorrectly stated that connected cars have not been compromised outside of a controlled setting.

Wide-scale malicious automobile hacking is no longer theoretical. The lower court failed to appreciate the nature and immediacy of the problem when it concluded that the threat is "speculative." Order 14–15. Although a full-scale remote car hijacking is certainly a serious risk to car owners and others—*see, e.g.*, Andy Greenberg, *Hackers Remotely Kill a Jeep On the Highway–With Me in It*, Wired (July 21, 2015)[18]—hijacking is not the only risk posed by connected car vulnerabilities. *See* Bruce Schneier, *The Internet of Things Will Turn Large-Scale Hacks Into Real World Disasters*, Motherboard (July 25, 2016)[19] (explaining that information systems face three threats: theft (i.e. loss of confidentiality), modification (i.e. loss of integrity), and lack of access (i.e. loss of availability)). Connected cars leave consumers open to car theft, data theft, and other forms of attack as well. These attacks are not speculative; many customers have already suffered due to vulnerable car systems.

For example, criminals have exploited vulnerabilities in connected cars to perpetrate car "ransomware" scams, "where a car is disabled by malicious code until a ransom is paid." Nora Young, *Your Car Can be Held for Ransom*,

---

[18] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[19] http://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.

CBCradio (May 22, 2016).[20] According to one expert, computer criminals have installed malicious software in cars via USB drives used by mechanics for diagnostics and software updates. *Id.* The software shuts down, or "bricks," the car unless and until the driver meets the criminal's demands. *Id.* The expert even discovered a case where an entire fleet of vehicles was disabled by ransomware. *Id.* She warns that criminals can also infect a car with malware remotely over the car's wireless connection. *Id.*

Car theft via the hacking of computer-based door locks has also become rampant. *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. Times (Apr. 15, 2015);[21] Andy Greenberg, *Radio Attack Lets Hackers Steal 24 Different Car Models*, Wired (Mar. 21, 2016);[22] Patrick J. Kiger, *How to Protect Your Car from Keyless-Entry Hacking*, Edmunds (Jan. 15, 2016).[23] Some sophisticated thieves have used laptops to decrypt a car key fob code in order to gain access. Bilton, *supra*; KHOU-TV, *Two Arrested for Stealing Jeeps – Using*

[20] http://www.cbc.ca/radio/spark/321-life-saving-fonts-ransomware-cars-and-more-1.3584113/your-car-can-be-held-for-ransom-1.3584114.
[21] http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.
[22] https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/.
[23] http://www.edmunds.com/car-technology/how-to-protect-your-car-from-keyless-entry-hacking.html.

Laptops, USAToday (Aug. 4, 2016).[24] In fact, in 2006, thieves used this technique to steal David Beckham's $100,000 BMW X5. *Id.* Other attackers use an "amplification attack" to "silently extend[] the range of unwitting drivers' wireless key fobs to open cars and even start their ignitions." Greenberg, *Radio Attack Lets Hackers Steal 24 Different Car Models*, *supra*. For less sophisticated thieves, hackers have developed an inexpensive device that can unlock many cars that have keyless entry. Cadie Thompson, *A Hacker Made a $30 Gadget That Can Unlock Many Cars That Have Keyless Entry*, Tech Insider (Aug. 6, 2015).[25]

Connected cars aren't only vulnerable to hacks of the CAN bus; these vehicles are also vulnerable because the car manufacturers themselves have access. Anyone who wants to infiltrate a large number of connected cars needs only to gain access to the manufacturer's credentials. In 2010, Omar Ramos-Lopez, a former Texas Auto Center employee, disabled more than 100 cars after being laid off. Kevin Poulsen, *Hacker Disables More than 100 Cars Remotely*, Wired (Mar. 17, 2010).[26] Ramos-Lopez used a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

[24] http://www.usatoday.com/story/money/cars/2016/08/04/two-arrested-auto-theft-jeeps----using-laptops/88280304/.
[25] http://www.techinsider.io/samy-kamkar-keyless-entry-car-hack-2015-8.
[26] https://www.wired.com/2010/03/hacker-bricks-cars/.

Id. Ramos-Lopez used another employee's account to gain access to the immobilization system. *Id.*

In fact, thieves recently stole a 2010 Jeep Wrangler from its owner's driveway, likely by gaining access to the dealer's tools. Jeff Bennett, *Thieves Go High-Tech to Steal Cars*, Wall St. J. (July 5, 2016).[27] Representatives of Fiat Chrysler explained that "an individual with access to a dealer website may have sold the information to a thief." *Id.* These vehicles are especially vulnerable not only because the CAN bus systems are insecure, but because the manufacturers have created a point of weakness that can allow hackers into the system.

Connected cars are also vulnerable to GPS spoofing: "the act of broadcasting a fake GPS signal to fool a device into thinking it's somewhere else, and/or at a different point in time." Guy Buesnel, *GPS Spoofing Is Now A Real Threat – Here's What Manufacturers of GPS Devices Need to Know*, Spirent (Sept. 14, 2015).[28] Low-cost GPS signal emulators can take control of the GPS receivers in car satellite navigations systems, allowing hackers to steer drivers off-course. *See id.*

The federal government, including law enforcement agencies, has recognized the threat posed by the vulnerabilities of connected cars. After research

[27] http://www.wsj.com/articles/thieves-go-high-tech-to-steal-cars-1467744606.
[28] http://www.spirent.com/Blogs/Positioning/2015/September/GPS_Spoofing_Is_a_Real_Threat.

showed that cars can be hacked remotely via their wireless connections, the FBI issued a Public Service Announcement warning that motor vehicles are increasingly vulnerable to remote exploits. FBI, *Motor Vehicles Increasingly Vulnerable to Remote Exploits*, Public Service Announcement I-031716-PSA (Mar. 17, 2016).[29] The FBI cautioned drivers that "[v]ulnerabilities may exist within a vehicle's wireless communication functions, within a mobile device—such as a cellular phone or tablet connected to the vehicle via USB, Bluetooth, or Wi-Fi—or within a third-party device connected through a vehicle diagnostic port." *Id.* Attackers would then be able to "remotely exploit these vulnerabilities and gain access to the vehicle's controller network or to data stored on the vehicle." *Id.* The FBI directed consumers to a website set up explicitly to receive consumer complaints of vehicle hacking. *Id.*

Although there have already been reports of highly sophisticated remote automobile attacks, it is important to consider that the coverage of these kinds of attacks is woefully incomplete. Manufacturers themselves don't even understand the scope of the problem. A report produced by U.S. Senator Edward Markey's office found that of the sixteen car manufacturers questioned, only five claimed to be able to detect wireless intrusions. Staff of Senator Edward J. Markey, 114th Cong., *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at*

[29] https://www.ic3.gov/media/2016/160317.aspx.

Risk 7 (Feb. 2015)[30] [hereinafter Markey Report]. But the fact that there is still much work to be done to understand these vulnerabilities does not undercut the plaintiffs' allegations.

C. Manufacturers should be obligated to implement safeguards to protect consumers from car hacking.

The risks posed by connected cars are serious, but techniques already exist to protect consumers; manufacturers should be required to implement these safeguards to protect their customers. Various agencies and organizations have offered solutions that would protect consumers from many of the typical attacks. The GAO recently reported that "a range of key practices are available to identify and mitigate potential cybersecurity vulnerabilities in vehicles." GAO Report, *supra*, at 20–25. These include techniques "used by other industries" such as "penetration testing and code reviews." *Id.* at 20. For example, security researchers have called for the installation of "intrusion-prevention device[s]" and "the use of code-signing technology to help make sure only valid code runs on cars." Sean Michael Kerner, *Car Hackers Return to Black Hat to Reveal New Flaws*, eWeek (Aug. 4, 2016).[31]

---

[30] https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[31] http://www.eweek.com/security/car-hackers-return-to-black-hat-to-reveal-new-flaws.html.

Even the manufacturers and their suppliers have acknowledged the need to implement safeguards. General Motors CEO Mary Barra recently declared that a "cyber incident is not a problem just for the automaker involved," but "is a problem for every automaker around the world" and "a matter of public safety." Will Knight, *GM CEO: Car Hacking Will Become a Public Safety Issue*, Tech. Review (July 22, 2016)[32] (internal quotation marks omitted). Intel, which provides various components to the automotive industry including hardware, software, and security processes, remains optimistic about the goal of "ensur[ing] the new vehicle paradigm is protected and can operate to its full potential, even in a malicious operating environment." Intel Sec., *Automotive Security Best Practices: Recommendations for Security and Privacy in the Era of the Next-Generation Car* (*Intel Report*) 4 (2015).[33] Intel outlined numerous ways in which car manufacturers can continue to innovate while still protecting consumers from malicious hackers. *Id.* Symantec, which provides data security products, has also articulated methods that car manufacturers can employ to safeguard consumers against various forms

[32] https://www.technologyreview.com/s/601957/gm-ceo-car-hacking-will-become-a-public-safety-issue/.
[33] http://www.intel.com/content/www/us/en/automotive/automotive-security-best-practices-white-paper.html.

of malicious hacking, while maintaining a high level of technological innovation. Symantec, *Building Comprehensive Security Into Cars* (Aug. 8, 2015).[34]

Car manufacturers should adopt data security measures. Early mitigation of threats to public safety may reduce auto fatalities, spur innovation, and result in safer vehicles. *See generally*, Ralph Nader, *Unsafe at Any Speed* (1965).

III. Car manufacturers collect a great deal of personal information about drivers.

Car manufacturers have designed modern vehicles to produce and record an enormous amount of personal information. Cars can even access and store the contents of the operator's cell phone through techniques that "sync" the phone with the car's onboard computer. *See* Ronald Montoya, *Car Technology and Privacy*, Edmunds (Feb. 12, 2013).[35] Manufacturers have access to this data, which includes the car's location and operational information, and the incident information generated by event data recorders ("EDRs"). Markey Report, *supra*, at 8.

The lower court erred by concluding, without explanation, that this data "is not categorically the type of sensitive and confidential information the [California] constitution aims to protect." Order 23. To the contrary, drivers have an

[34] http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf.
[35] http://www.edmunds.com/car-technology/car-technology-and-privacy.html.

informational privacy right in "precluding the dissemination or misuse" of driver data that the manufacturers have obtained.

Information provided by the manufacturers themselves help demonstrate the scope of data collection that occurs. Named plaintiffs Helene Cahen and Merrill Nisam purchased a Lexus RX 400 H in 2008 and a Chevrolet Volt in 2013, respectively. Order 3. The manufacturers of both of these cars have acknowledged that they collect a great deal of information about drivers' activities, including operational data and the incident data from EDRs. This driver data is linked to the car and identifiable to the driver unless it has been properly anonymized.

The computer systems embedded in connected cars "record information about the vehicle's performance and how it is driven." Chevrolet, *2013 Chevrolet Volt Owner Manual* 370 (2013)[36] [hereinafter 2013 Volt Manual]. For example, the "vehicle data recordings" for the Chevrolet Volt include:

- "[E]ngine and electric drive unit performance";
- The "conditions for airbag deployment";
- Antilock braking;
- "[H]ow the vehicle is operated, such as rate of fuel consumption or average speed"; and

[36] https://www.chevrolet.com/content/dam/Chevrolet/northamerica/usa/nscwebsite/en/Home/Ownership/Manuals_and_Videos/02_pdf/2k13volt.pdf.

- "[P]ersonal preferences, such as radio presets, seat positions, and temperate settings."

Id. The Volt "infotainment" navigation system can also collect "destinations, addresses, telephone numbers, and other trip information." *Id.* at 372; *see also* Chevrolet, *2016 Chevrolet Volt Owner Manual* 345, 346 (2016).[37]

The Lexus RX 350 is similarly "equipped with several sophisticated computers" that record:

- Engine speed;
- Accelerator status;
- Brake status;
- Vehicle speed; and
- Shift position.

Lexus, *2016 Lexus RX 350 Owner's Manual* 9 (2016)[38] [hereinafter 2016 Lexus Manual]. The amount of data collected by Lexus has also been increasing over time. For example, while the 2008 Lexus RX 400H manual did not explicitly mention vehicle data recordings, *see* Lexus, *2008 Lexus RX 400H Owner's Manual*

[37] https://my.chevrolet.com/content/dam/gmownercenter/gmna/dynamic/manuals/2016/Chevrolet/Volt/2k16volt1stPrint.pdf.
[38] https://carmanuals2.com/lexus/rx350-2016-owner-s-manual-81315.

(2008) [hereinafter 2008 Lexus Manual], the 2016 manual includes a detailed list of driver data collected by the company, 2016 Lexus Manual, *supra*, at 9.

Modern cars also include built-in EDRs, which are separate devices installed to "record technical vehicle and occupant information" in the seconds before, during, and after an incident or crash. Nat'l Highway Traffic Safety Admin., *Welcome to the NHTSA Event Data Recorder Research Web site*.[39] EDRs "may record (1) pre-crash vehicle dynamics and system status, (2) driver inputs, (3) vehicle crash signature, (4) restraint usage/deployment status, and (5) post-crash data such as the activation of an automatic collision notification (ACN) system." *Id*. EDR data is so sensitive that Congress and 17 states have enacted laws to limit data retrieval from EDRs. *See* Driver Privacy Act of 2015, Pub. L. No. 114-94, Title XXIV, Subtitle C, Pt. I, 129 Stat. 1312, 1712–13; Nat'l Conference of State Legislatures, *Privacy of Data From Event Data Recorders: State Statutes* (Jan. 4, 2016).[40]

The Chevrolet and Lexus cars at issue in this case are both equipped with EDRs that collect detailed information about the car and driver, including:

- Gasoline engine speed;

[39] http://www.nhtsa.gov/Research/Event+Data+Recorder+(EDR)/Welcome+to+the+NHTSA+Event+Data+Recorder+Research+Web+site (last visited Aug. 1, 2016).

[40] http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

- Whether or how far the brake pedal was applied;
- Vehicle speed;
- How far the accelerator pedal was depressed;
- Position of the transmission shift lever;
- Whether the driver and front passenger wore seat belts;
- Driver's seat position;
- Front passenger's occupant classification;
- Supplemental Restraint System airbag deployment data;
- Supplemental Restraint System airbag system diagnostic data; and
- How various systems in the vehicle were operating.

2008 Lexus Manual, *supra*, at 394–95; 2013 Volt Manual, *supra*, at 370–71.

Lexus states that it collects and uses vehicle data for "research purposes," but claims that "the data is not tied to a specific vehicle or vehicle owner." 2016 Lexus Manual, *supra.* Both GM and Toyota use consumer EDR data for research purposes when "necessary," and can disclose that data to third parties for research purposes. 2008 Lexus Manual, *supra*, at 395; *accord.* 2013 Volt Manual, *supra*, at 371. Both companies claim that they use and disclose the EDR data not tied to a "vehicle owner." 2013 Volt Manual, *supra*, at 371; 2008 Lexus Manual, *supra*, at 395.

But there is currently no evidence to show that the driver data collected by these cars is properly anonymized. Data about the location, operation, and conditions of a vehicle is linked to the driver and should be subject to the same privacy protections as other sensitive, personal information.

Companies that claim to deal only in "anonymous" data, "do not mean that they have no way to distinguish a specific person," or that "they have no way to recognize [the user] as the same person with whom they have interacted previously." Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent*, *in Privacy, Big Data, and the Public Good* 44, 53 (Julia Lane et al. eds. 2014). Rather than properly anonymize data, many companies simply "rely on unique persistent identifiers that differ from those in common and everyday use (i.e. a name and other so-called personally identifiable information)." *Id.* The widespread use of the Social Security Number ("SSN") illustrates the privacy impact of linking data with a unique persistent identifier even if that identifier consists only of numbers. On its own, a SSN is nothing more than a nine-digit number. Large institutions, however, frequently use SSNs for identification because they are "necessarily more unique than given names, the more common of which (e.g. John Smith) could easily recur multiple times in the same database." *Id.* at 54.

So too with vehicle- or driver-specific identifiers, which would be linkable to an individual without needing to use her actual name or vehicle identification number. Even seemingly "anonymous" driving data can act as a unique "driver fingerprint[t]." Miro Enev, Alex Takakuwa, Karl Koscher, & Tadayoshi Kohno, *Automobile Driver Fingerprinting*, 2016(1) Proceedings on Privacy Enhancing Techs. 34 (2016);[41] Andy Greenberg, *A Car's Computer Can 'Fingerprint' You in Minutes Based on How You Drive*, Wired (May 25, 2016).[42] In a recent study, researchers uniquely distinguished drivers based on data from "16 sensors that already broadcast over the car's internal computer network," including brake pedal position, steering wheel angle, fuel consumption rate, and turn signal. *Automobile Driver Fingerprinting*, *supra*, at 35, 40. Using 15 sensors and the database of driving data, the researchers differentiated between 15 drivers with 100% accuracy. *Id.* at 35. The researchers also achieved 100% accuracy using just the brake pedal and the entire dataset for training, 99% accuracy using the top five sensors, and 87% accuracy using just the brake pedal and the first 15 minutes of open-road driving as a training database. *Id.*

In order to avoid the risk of disclosure of personal driver data, aggregate statistical data must go through a process of "de-identification." De-identification

[41] http://www.autosec.org/pubs/fingerprint.pdf.
[42] https://www.wired.com/2016/05/drive-car-can-id-within-minutes-study-finds/.

"refers to the process of removing or obscuring any personally identifiable information from [records] in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them." Privacy Tech. Assistance Ctr., U.S. Dep't of Educ., *Data De-identification: An Overview of Basic Terms* 2–3 (2013)[43]. But even de-identified data should only be collected and disclosed with caution, because seemingly "anonymous" data can be made identifiable. *See, e.g.*, Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., FTC, to Reed Freeman, Counsel for Netflix, Inc. (Mar. 12, 2010)[44] (discussing how two researchers identified individual Netflix users from a data set of "anonymized" customer view data).

Without knowing more about how the defendant car manufacturers collect and use the plaintiffs' personal driver data, the lower court was wrong to find definitively that the data collected "is not categorically the type of sensitive and confidential information the constitution aims to protect." Order 23. Indeed, the U.S. Supreme Court has recently recognized substantial privacy interests in the "long-term monitoring" of a vehicle's movements, *United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of

[43] http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf.
[44] https://www.ftc.gov/sites/default/files/documents/closing_letters/netflix-inc./100312netflixletter.pdf.

privacy.") and in the digital information located on cell phones, *Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473, 2489–91 (2014) ("Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.").

* * *

Connected vehicles raise significant public safety concerns that the courts cannot ignore. One company has already recalled 1.4 million vehicles because of the risk of remote hacking. Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*, Wired (July 24, 2015).[45] "Almost twenty states have taken steps to regulate the collection and use of driver data. So far, researchers and scientists in controlled settings have done most of the reported hacks of moving cars. But wide scale malicious automobile hacking is certainly imminent, if not already occurring." *The Internet of Cars: Hearing Before the H. Subcomm. on Info. Tech and the H. Subcomm. on Transp. and Pub. Assets of the H. Comm. on Oversight and Gov't Reform*, 114th Cong. (2015) (statement of Khaliah Barnes, EPIC Associate Director and Administrative Law Counsel).[46]

[45] https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.
[46] https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf.

CONCLUSION

EPIC respectfully requests that this Court vacate the lower court's order.

August 5, 2016

Respectfully submitted,

/s/ Alan Butler

Marc Rotenberg
Alan Butler
Aimee Thomson
Electronic Privacy Information Center
1718 Connecticut Ave. N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 6,252 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word for Mac 2011 in 14 point Times New Roman style.

/s/ Alan Butler

Dated: August 5, 2016 Alan Butler

CERTIFICATE OF SERVICE

I hereby certify that on August 5, 2016, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ Alan Butler

Dated: August 5, 2016 Alan Butler