INVISIBLE, BUT NOT TRANSPARENT: AN ANALYSIS OF THE DATA PRIVACY ISSUES THAT COULD BE IMPLICATED BY THE WIDESPREAD USE OF CONNECTED VEHICLES

By Emilio Longoria[1]

2017

ABSTRACT

In 2015, the U.S. Department of Transportation began the first phase of its 50-month program to introduce connected vehicles to American roadways. While many have focused on the potential traffic safety benefits wide-scale implementation of connected vehicle technology could ultimately bring about, few have discussed the potentially serious data privacy issues that connected vehicles could create. Although few know the exact

[1] Emilio Longoria received a B.A. in History from Rice University in 2013 and a J.D. from the University of Texas School of Law in 2017. Since September of 2017, he has worked as an associate at Norton Rose Fulbright LLP in Houston, Texas. During the 2018-19 term, Emilio will clerk for the Hon. George C. Hanks, Jr. of the Southern District of Texas. Emilio would like to thank his family and friends for all their love and support—without them this article would not have been possible.

technological capabilities connected vehicles will have, it is likely that they will be designed to regularly transmit highly sensitive private information over a relatively unsecure network. This paper analyzes the potential privacy issues that could be implicated by such a system, with particular focus as to how those issues are exacerbated by existing state law. Unless substantial amendments are made to existing legislative schemes, widespread use of connected vehicles could seriously jeopardize the security of our private information.

ABSTRACT 1
A SNAKE IN THE GRASS: AN ANALYSIS OF THE DATA PRIVACY ISSUES THAT COULD BE IMPLICATED BY THE WIDESPREAD USE OF CONNECTED VEHICLES 3
INTRODUCTION 3
I. WHAT TYPES OF DATA WILL CVS HAVE THE ABILITY TO COLLECT? 6
II. WHAT KIND OF DATA IS A CV CAPABLE OF TRANSMITTING, AND WHO CAN IT TRANSMIT THAT DATA TO? 11
III. LEGAL ISSUES THAT ARE CREATED BY THE DATA TRANSMISSION CAPABILITIES OF CVS, AND HOW EXISTING LAWS AND RULES MAY NOT BE ADEQUATELY PROTECTIVE OR COULD EVEN EXACERBATE THESE ISSUES. 14
1. Data Privacy Issues Implicated by V2V Communications. 15
2. Data Privacy Issues Implicated by V2I Communications. 17
3. Data Privacy Issues Implicated by Communications between CVs and Independent Commercial Businesses. 19
IV. STATE LAWS THAT ATTEMPT TO GRAPPLE WITH THE PRIVACY ISSUES IMPLICATED BY WIDESPREAD CV USE, AND THEIR INABILITY TO DO SO COMPLETELY. 21
1. State Data Breach Laws 22
2. Motor Vehicle Disclosure Acts 24
3. Laws Regulating Electronic Device Recorders 26
V. PRELIMINARY SUGGESTIONS FOR HOW EXISTING STATE LAWS COULD BE AMENDED IN ORDER TO GRAPPLE WITH SOME OF THE PRIVACY ISSUES IMPLICATED BY THE CV DATA TRANSMISSION SCHEME. 28
1. Updating Key Language in Current State Laws

Impacting Disclosures of Private Information 29
2. Placing Restrictions on the Subsequent use of Information Obtained through Open Records Acts. . 33
3. Amending Data Breach Laws by Placing an Affirmative Duty on State governments to Disclose to CV Participants when their Personal Information is Collected by the State, and to Explain what type of Information was Collected..... 35
CONCLUSION..... 37

A SNAKE IN THE GRASS: AN ANALYSIS OF THE DATA PRIVACY ISSUES THAT COULD BE IMPLICATED BY THE WIDESPREAD USE OF CONNECTED VEHICLES

INTRODUCTION

Experts predict that the use of automated and connected vehicles will be "increasingly common" in U.S. markets between 2025 and 2030.[2] While many are excited by the reduction of auto accidents,[3] and the increase in productivity[4] that this may cause, some are also concerned by the privacy issues that could be implicated by the widespread operation of driverless vehicles throughout the United States.[5] One specific concern, and the focus of this paper, is the question of who owns the highly sensitive private information that connected vehicles ("CV") have the ability

[2] JAMES ANDERSON ET AL., AUTONOMOUS VEHICLE TECHNOLOGY: A GUIDE FOR POLICYMAKERS 57 (2016).

[3] Bec Crew, *Driverless Cars Could Reduce Traffic Fatalities by Up to 90%, Says Report*, SCIENCE ALERT (Oct. 1, 2015), http://www.sciencealert.com/driverless-cars-could-reduce-traffic-fatalities-by-up-to-90-says-report.

[4] Craig Thomas, *Driverless Cars Could Save Families £3,000 a Year*, SUNDAY EXPRESS (May 30, 2016), http://www.express.co.uk/life-style/cars/675065/Driverless-cars-could-save-families-thousands-of-pounds-a-year ("[D]riverless motoring would cut journey times by 50%, with motorists gaining about two hours of extra free time per day.").

[5] *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1172 (2012) (discussing surveillance issues); *see also* Bryant Walker-Smith, *Proximity-Driven Liability*, 102 GEO. L.J. 1777, 1820 (2014) (discussing general privacy issues).

to collect[6] and disseminate to state agencies[7] and possibly to private third parties[8] via the government-owned-and-operated dedicated short-range communications system currently used for CV transportation.[9]

A technically distinct form of motor vehicle operation from an autonomous vehicle, a CV navigates the roadways by communicating with (1) other CVs on the road[10] and (2) with state-owned sensors physically embedded in the infrastructure of the road the CV is driving on.[11] As opposed to the autonomous vehicle, which navigates roadways chiefly through the use of complex radar equipment that identifies any roadway obstacle,[12] the CV relies on data exchanges with its environment and other driver's around it in order to safely transport its passengers.[13] Although any particular motor vehicle can be outfitted with both CV and autonomous vehicle technology,[14] it is the information exchanges required for a functioning CV system that this paper is concerned with, in large part, because the information exchanges inherent in CV operation are not already governed by privately negotiated data user agreements, as they are in autonomous vehicle operation.[15]

---

[6] *See* Dorothy J. Glancy et al., *A Look at the Legal Environment for Driverless Vehicles,* 69 LEGAL RES. DIG. 3, 20 (Feb. 2016) (explaining that driverless vehicles are likely to have the ability to collect biometric and personality data).

[7] *See* Enoch R. Yeh, et al., *Security in Automotive Radar and Vehicular Networks*, MICROWAVE JOURNAL (2016), http://www.caee.utexas.edu/prof/bhat/ABSTRACTS/SecurityOverview_mmWave_V2X.pdf (explaining that driverless cars will be able to communicate with sensors owned by the state embedded in the physical infrastructure).

[8] *Legal Environment for Driverless Vehicles*, *supra* note 6, at 24 ("[T]he FCC is under Congressional pressure to re-allocate parts of the now-dedicated 5.9 GHz DSRC spectrum to other types of wireless users.").

[9] Dorthy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J. 1617, 1627–28 (2015).

[10] *Connected Vehicle Challenges: Potential Impact of Sharing the 5.9 GHz Wireless Spectrum*, U.S. DEP'T OF TRANSP., http://www.its.dot.gov/cv_basics/pdf/CV_basics_DSRC_factsheet.pdf ("Connected vehicles use secure and anonymous wireless technology to communicate with other vehicles, road infrastructure, and personal mobile devices.").

[11] *Id.*

[12] *Legal Environment for Driverless Vehicles*, *supra* note 6, at 21 ("Multiple forms of radar, LIDAR, infrared, sonar, and optics (digital cameras) combine to provide a detailed and robust 'picture' of the immediate and farther away roadway environment.").

[13] *Id.*

[14] Siva R. K. Narla, *The Evolution of Connected Vehicle Technology: From Smart Drivers to Smart Cars to . . . Self-Driving Cars*, ITE J. 22, 22 (2013).

[15] *See* Walker-Smith, *supra* note 5, at 1790 (explaining that the user

As can be imagined, the constant swaps of private information a CV participates in over the normal course of operation creates tricky and novel questions concerning data ownership and use not presented by autonomous vehicles. These questions are made trickier when taking into account the types of information that a CV can collect[16] and the fact that CVs are designed to regularly transmit that information to government agencies and third parties.[17] For example, if a CV transfers information concerning its passengers to a state-owned highway sensor, is that information now retained by the sensor subject to an open records request under the reasoning that it is state highway information? And, when a CV transmits information to a second CV while passing it on the road, is the second CV owner entitled to use that information for any purpose?[18] These challenges do not arise with autonomous vehicles because autonomous vehicles are not designed to constantly exchange information with government agencies or lay third parties; rather, the information swaps in which autonomous vehicles take part are with satellites and mapping programs owned or licensed by the vehicle's manufacturer and therefore governed by user agreements.[19]

This paper will attempt to grapple with the privacy issues implicated by the CV data transmission scheme by (I) explaining the types of private information driverless cars are expected to

---

agreements created by the manufacturers of driverless cars usually provide that the manufacturer has a "royalty-free, fully paid . . . perpetual license" that entitles it to use any data the driverless car collects. However, this paper is concerned with the limits that must be placed on private information transferred to private third-parties and the government via the CV functions of a driverless car, which CV operators are not in privity of contract with.).

[16] *See id.* at 1782–83 (discussing the ability of future driverless cars to use existing technology to collect biometric and personality data).

[17] *See* Jack Boeglin, *The Costs of Self-Driving Cars: Reconciling Freedom and Privacy with Tort Liability in Autonomous Vehicle Regulation*, 17 YALE J.L. & TECH. 171, 198 (2015) (discussing vehicles designed to communicate in a manner that does not protect the user's freedom or privacy).

[18] *See FCC Allocates Spectrum in 5.9 GHz Range for Intelligent Transportation Systems Uses*, FED. COMM. COMMISSION (Oct. 21, 1999), https://transition.fcc.gov/Bureaus/Engineering_Technology/News_Releases/1999/nret9006.html (discussing why the FCC had assigned 75 MHz of spectrum at 5.850-5.925 GHz—often referred to as the 5.9 GHz spectrum—solely for vehicle safety and mobility communications over DSRC in 1999. These questions are further complicated by the fact that the short-range communications system that CVs use to transfer information is owned and operated by the federal government.).

[19] *See* Harry Surden & Mary-Anne Williams, *Technological Opacity, Predictability, and Self-Driving Cars*, 38 CARDOZO L. REV. 121, 138 (Aug. 12, 2016) (discussing the use of satellites by autonomous vehicles).

have the physical capability to collect; (II) discussing the platform by which CVs will have the ability to transmit that information and who may have access to that platform; (III) identifying the legal issues that are created by CV data transmission capabilities with particular focus on how existing laws and rules may not be adequately protective or could even exacerbate challenges to privacy through mandated disclosure laws; (IV) examining the ability of existing state laws to provide some answers as to the limits of use of information received from CVs; and (V) provide preliminary suggestions for how existing state laws could be amended in order to grapple with some of the privacy issues implicated by the CV data transmission scheme.

Research and investment in driverless car technology is at an all-time high,[20] and because of large federal investments in CV transportation infrastructure nationwide,[21] the privacy issues implicated by widespread CV use are likely to require immediate answers. Therefore, the privacy issues that widespread operationalization of CVs entails need to be identified and considered. Further, while existing state law provides initial responses to some of these questions, it seems that answers to most of these questions will require either new legislation, or heavy editing to some of the privacy laws that are already on the books.

I. WHAT TYPES OF DATA WILL CVS HAVE THE ABILITY TO COLLECT?

In order to understand what kinds of privacy concerns could be implicated by the permeation of CVs into American markets, it is necessary to comprehend the types of information CVs have the ability to collect and the manner in which they can store that data. In this regard, distinguishing between CVs and autonomous vehicles is no longer helpful, because, as mentioned, driverless cars are usually outfitted with both technologies,[22] and therefore

---

[20] *See* Autotech, *44 Corporations Working On Autonomous Vehicles*, CB INSIGHTS (Mar. 18, 2017), https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/ (listing the corporations involved in producing and enhancing self-driving vehicles).

[21] *See US Government Gets in Gear by 'Investing' in Connected Cars*, TU-AUTOMOTIVE (July 6, 2015), http://analysis.tu-auto.com/autonomous-car/us-government-gets-gear-investing-connected-cars ("The USDOT has funded connected vehicle infrastructure in '[a] number of localities in different parts of the US,' investing between '$100,000' to '$20M' per site.").

[22] William J. Kohler & Alex Colbert-Taylor, *Current Law And Potential Legal*

both CVs and autonomous cars have virtually indistinguishable capabilities to collect data. It is also important to note at the outset of this section that although many resources identify the types of information current CV models can collect, the limits of CV technology are relatively unknown.[23] Therefore, this article merely presents a "best guess" as to the types of information CVs will collect, based on what currently available resources hypothesize will be the limits of CV collection.

Highly similar in appearance to modern motor vehicles,[24] CVs are expected to be relatively indistinguishable from non-connected cars on the road.[25] However, under their familiar frame exists a highly complex and novel technological infrastructure designed to collect and disseminate information.[26] According to a recent report, a new CV "may have more than 145 actuators and 75 sensors, which produce more than 25 GB of data per hour. The data is analyzed by more than 70 onboard computers to ensure safe and comfortable travel."[27] To put this piece of information into perspective, that would give a CV the computing power to collect "about a dozen HD movies" worth of information an hour.[28]

With respect to the types of information CVs will have the ability to collect, the Department of Transportation has released a list of 18 categories of data that CVs are currently collecting in pilot transportation programs throughout the United States, which is illustrative of the current capabilities of CVs in this regard.[29]

Issues Pertaining To Automated, Autonomous And Connected Vehicles, 31 SANTA CLARA HIGH TECH. L.J. 99, 103 (2015) ("The authors of the present article believe that the development of dependable [autonomous and connected vehicle] technology . . . and the convergence of these categories, will be a necessary precursor to the commercial introduction of substantially autonomous vehicles.").

[23] *See id*. at 104 (discussing the uncertainty around how connected and autonomous vehicle technology will advance in the future).

[24] Dorothy J. Glancy, *Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem,* 16 MINN. J.L. SCI. & TECH. 619 (2015).

[25] Russ Mitchell, *Driverless Cars Won't Always Look This Way,* LOS ANGELES TIMES (Feb. 17, 2017), http://www.latimes.com/business/autos/la-fi-hy-driverless-cars-appearance-20160914-snap-story.html.

[26] *Automous and Automated and Connected Cars*, *supra* note 24, at 621.

[27] *Legal Environment for Driverless Vehicles*, *supra* note 6, at 31.

[28] Hitachi, *Connected Cars Will Send 25 Gigabytes of Data to the Cloud Every Hour*, QUARTZ, https://qz.com/344466/connected-cars-will-send-25-gigabytes-of-data-to-the-cloud-every-hour/.

[29] *Research Data Exchange*, U.S. DEP'T OF TRANSP., https://www.its-rde.net/index.php/data/searchdata. The 18 categories of data are: loop data, volume, speed, occupancy, location metadata, incidents, weather, signal, travel time, transit, lane closures, vehicle location, onboard equipment, roadside

Primarily dealing with routine traffic operation, examples of some of these categories of data include: (1) a vehicle's speed at distinct intervals; (2) a vehicle's geographic location; and (3) any traffic signals emitted by the CV (e.g. hazard lights, turn signal).[30]

Moreover, experts have identified several other types of data CVs could collect within the coming years that could be considered even more sensitive than the types of data currently being collected in CV pilot programs.[31] Specifically, these are biometric data—like a CV operator's voice samples and fingerprints,[32] a CV operator's driving personality,[33] and passenger manifests of anyone traveling in the CV.[34] And this is not even taking into account the ability CVs may have in the future to integrate intrusive data collection strategies currently being operationalized in different commercial industries.[35] For example, Google now owns "a small biometric firm . . . that has developed face recognition, video tracking and recognition, and face-based soft-biometric technologies,"[36] which could possibly be used in CVs.[37] And Microsoft's Kinect, "designed for its Xbox and loved by researchers, 'can monitor users' movements with a camera that sees in the dark, picks up voice commands with a microphone, and reads your heart rate using infrared cameras that track blood flow underneath the skin"[38]—which could also be integrated into future CV models.[39] To put it bluntly, CVs are literally being designed to

---

equipment, simulation, live data, basic safety message, and queue length.

[30] *Id.*

[31] *Legal Environment for Driverless Vehicles*, *supra* note 6, at 20.

[32] *Id.*

[33] *Id.* For example, the CV may collect data on whether someone likes to drive aggressively and speed or whether a passenger wants to take the most scenic route.

[34] *See* Barry Devlin, *Autonomous Vehicles: A World of New Data and Analytics (Part 2 of 4)*, TDWI (July 12, 2016), https://tdwi.org/Articles/2016/07/12/Autonomous-Vehicles-World-of-New-Data-Pt2.aspx?Page=2. In the case of an accident or crime, the CV may be able to communicate who is in the car and identifying information about that person.

[35] *See* Walker-Smith, *supra* note 5, at 1782 (explaining that companies use savvy methods of data collection to decipher information about consumers); *see also Legal Environment for Driverless Vehicles*, *supra* note 6, at 1214 (explaining that if security measures are not taken to protect data, this data can be used to profile, predict, and possibly manipulate vehicles and their users).

[36] Walker-Smith, *supra* note 5, at 1783.

[37] *Id.*; *see also Legal Environment for Driverless Vehicles*, *supra* note 6, at 20 (explaining that driverless vehicles may contain biometric interfaces).

[38] Walker-Smith, *supra* note 5, at 1783.

[39] Damon Lavrinc, *Kinect in Cars? Microsoft Job Listing Hints at New Auto Application,* WIRED (June 26, 2012), https://www.wired.com/2012/06/kinect-in-

have the ability to collect "data about everything."[40]

Not only are CVs expected to have the ability to collect a diverse set of personal information, but they are also expected to have the ability to store that data for seemingly unlimited periods of time.[41] While storage on the hard drive actually embedded in a CV may be limited by design,[42] CVs are manufactured to constantly upload the information they collect to off-site data servers for future use.[43] Some predict that a standard CV would be able to upload as much as 25 GB of data an hour of such data to one of these off-site servers.[44] These off-site servers are not your typical servers either, as these machines would be highly sophisticated and designed to allow for the perpetual use of the information collected by a CV.[45] In fact, some sophisticated automotive manufacturers have already announced their plans to build new facilities dedicated to store and analyze all of the information collected by a CV in its normal course of operation.[46]

The government-owned-and-operated sensors that are designed to communicate with CVs, already embedded in our transportation infrastructure, are also expected to have a similar ability to store information.[47] As discussed, government servers are already

---

cars/. A job listing posted by Microsoft states that for the next generation of connected cars, Microsoft plans to include the "full power of the Microsoft ecosystem including Kinect."

[40] Hitachi, *supra* note 28.

[41] Shamik Ghosh, *Every Connected Car Will Send 130TB of Data to Cloud Per Year in Future: ACTIFIO,* TELEMATICS WIRE (Dec. 4, 2015), http://telematicswire.net/every-connected-car-will-send-130tb-of-data-per-year-in-future-actifio/. Experts predict that CVs will send 25 GB of data per hour to cloud storage, allowing for 130 TB of primary storage data per car per year.

[42] *See Nissan Leaf Customer Disclosure Form*, NISSAN, https://owners.nissanusa.com/content/techpub/ManualsAndGuides/NissanLEAF/2013/2013-NissanLEAF-Customer-Disclosure-Form.pdf ("The Nissan LEAF is equipped with several data recorders. . . . The EDR records data related to vehicle dynamics and safety systems for a short period of time, typically 30 seconds or less.").

[43] *See* Hitachi, *supra* note 28 ("Twenty-five gigabytes: that's how much data a connected car will upload to the cloud every hour").

[44] *Id.*

[45] *Id.* CVs upload data every hour and "have about 40 microprocessors and dozens of sensors," that can relay information about telematics and driver behavior, in addition to providing traffic and roadway feedback to cities and states.

[46] Yevgeniy Sverdlik, *Toyota to Build Data Center for Connected-Car Data*, DATA CENTER KNOWLEDGE (Jan. 4, 2016), http://www.datacenterknowledge.com/archives/2016/01/04/toyota-to-build-data-center-for-connected-car-data/.

[47] Kelsey Campbell-Dollaghan, *10,000 NYC Vehicles Are Going To Test the Government's Connected Car Tech,* GIZMODO (Sept. 14, 2015), https://gizmodo.com/10-000-nyc-vehicles-are-going-to-test-the-governments-c-1730653849.

collecting 18 different types of driver information in pilot programs throughout the country.[48] This has already led to the collection of reams of driver-related data[49] in at least 13 different cities[50]—and the size of this pilot program is only expected to grow.[51] As the U.S. Department of Transportation phrased it in one of the factsheets it published regarding the progress that has been made in CV pilot programs around the nation, the intelligent transportation system pilot program is dedicated to adopting "automation-related technologies as they emerge" and integrating them into the CV system for future use.[52]

The seemingly limitless ability CVs and government-owned sensors will have to collect private information underscores the privacy concerns that could be implicated by widespread CV use. If CVs are able to penetrate the American transportation market to the same degree as common automobiles, an army of around 250 million[53] CVs could be operating on American roads, collecting data as sensitive as vehicle occupancy, operator fingerprints, vehicle location, and occupant heart rate—and transmitting that data to other privately owned CVs or government-owned sensors.[54] Therefore, the high number of data exchanges inherent in a CV operation may mean access to previously inaccessible sensitive information by undesired parties. Moreover, because of the

---

[48] *Research Data Exchange*, *supra* note 29.

[49] *See Research Data Exchange: Portland*, U.S. DEP'T OF TRANS., https://www.its-rde.net/index.php/rdedataenvironment/10002 (showing an example of data collected in one U.S. city).

[50] *Research Data Exchange*, *supra* note 29. The 13 cities are: Portland, OR; San Diego, Calif.; Ann Arbor, Mch.; Seattle, Wash.; Orlando, Fla.; Pasadena, Calif.; Leesburg, Va.; Detroit, Mich., Columbus, Ohio; Los Angeles, Calif.; Emeryville, Calif.; Atlanta, Ga.; Sykesville, Md.

[51] Ellie Zolfagharifard, *Self-driving Cars Could be in 30 US Cities by 2017: Pilot Project Aims for Mass Roll Out of Driverless Vehicles - but How Safe are They?* DAILY MAIL (last updated Mar. 6, 2015), http://www.dailymail.co.uk/sciencetech/article-2981946/Self-driving-cars-30-cities-2017-Pilot-projects-aims-mass-roll-driverless-vehicles-safe-they.html.

[52] *ITS Strategic Plan 2015-2019*, U.S. DEP'T OF TRANS., http://www.its.dot.gov/factsheets/pdf/ITS_JPO_StratPlan.pdf.

[53] *See Questions & Answers: About DOT's Safety Pilot "Model Deployment,"* U.S. DEP'T OF TRANSP., https://www.its.dot.gov/factsheets/pdf/Technical_FactSheet_Model_Deployment.pdf (observing that currently, there are around 3,000 CVs operating on American roads).

[54] *See* Jerry Hirsch, *253 Million Cars and Trucks on U.S. Roads; Average Age is 11.4 Years*, LOS ANGELES TIMES (June 9, 2014), http://www.latimes.com/business/autos/la-fi-hy-ihs-automotive-average-age-car-20140609-story.html (using the number of currently operating motor vehicles as an example of the number of CVs that could operate on American roadways).

capability for CVs and the state to store all of the data they collected or received from CVs for perpetual use, there is unlikely to be any quick fix for these issues.

II. WHAT KIND OF DATA IS A CV CAPABLE OF TRANSMITTING, AND WHO CAN IT TRANSMIT THAT DATA TO?

Although CVs may have the ability to collect a wide range of data about their operators, it is impossible to accurately diagnose the privacy issues that will be implicated by widespread CV use without understanding the actual technological ability CVs have to transmit that information, and to whom they can transmit it.[55] Accordingly, it is necessary to discuss the extent, manner, and parties to which CVs are likely to disseminate information in order to grasp the range of privacy issues at stake.

Unlike your grandfather's car, the computers integrated into CVs are expected to have the capability to collect and disseminate information (1) between other privately owned CVs on the road;[56] (2) between the CV and state-owned sensors physically embedded in the infrastructure of the road the CV is driving on;[57] and perhaps (3) between the CV and independent commercial businesses.[58] Currently, independent commercial businesses are unable to access the network through which CVs communicate, but "the Federal Communications Commission (FCC) is under Congressional pressure to re-allocate parts of the now-dedicated [communications] spectrum" that CVs currently use to communicate "to other types of wireless users."[59] Therefore, this reality may change fairly soon.

CV information exchanges are currently made[60] through a

---

[55] Amadou Diallo, *Is Your Car a Privacy Threat?* FORBES (Dec. 16, 2013) https://www.forbes.com/sites/amadoudiallo/2013/12/16/connected-car-data-privacy/#527a9dac43db.

[56] Yeh, *supra* note 7.

[57] *Id.*

[58] *See Legal Environment for Driverless Vehicles*, *supra* note 6, at 23 (explaining the connectivity potential of CVs).

[59] Dorothy J. Glancy, *Legal Outlook for Autonomous, Automated, and Connected Cars,* FED'N OF DEFENSE & CORPORATE COUNSEL (July 25 to Aug. 1, 2015), https://c.ymcdn.com/sites/www.thefederation.org/resource/resmgr/Events/PastConferences/2015_Annual_Handouts.pdf.

[60] As I mentioned above, CV pilot programs are already in operation throughout the U.S.; therefore, CV technology is already in use. However, there is no expectation that the network through which CVs communicate will change anytime in the near or distant future.

dedicated short-range communications system ("DSRC") that operates on a 5.9 GHz spectrum, which the Federal Communications Commission ("FCC") has "set aside" for CVs to test the government's "highway auto-safety initiatives."[61] This means that, as of today, the networks through which CVs communicate can only be accessed by state-operated transportation agencies and individual CVs.[62] Therefore, although this may change significantly in the near future,[63] the players implicated in CV data transmission issues are fairly limited.

A highly sophisticated "next-generation"[64] communication network, the relatively uncongested DSRC network that CVs operate through allows for a "very high data transmission [rate]" of information with "low latency."[65] Specifically, the DSRC network can sustain the transmission of up to 27 MB of data per second, which is comparable to currently available domestic wireless Internet plans.[66] Accordingly, just like your computer at home, this means that the DSRC hardware empowers CVs to transmit almost any of the information they have the ability to collect in their normal course of operations.[67] Whether that be a photo, a fingerprint, or real-time GPS location data, it does not appear that the type of data that a CV transmits will be limited in any way by the actual network or hardware CVs use in order to communicate.[68]

---

[61] Melanie Zanona, *Automakers Push to Protect Spectrum for WiFi Connected Vehicles*, THE HILL (May 5, 2016), http://thehill.com/policy/transportation/278880-automakers-push-to-protect-wireless-reserved-for-connected-vehicles.

[62] *See id*. (explaining that the 5.9 GHz DSRC spectrum is currently reserved for highway safety initiatives).

[63] *See Legal Environment for Driverless Vehicles*, *supra* note 6, at 24 ("[T]he FCC is under Congressional pressure to re-allocate parts of the now-dedicated 5.9 GHz DSRC spectrum to other types of wireless users.").

[64] *Connected Vehicle Challenges*, *supra* note 10.

[65] *Id*.

[66] *See Dedicated Short Range Communications Spectrum Sharing and Operational Testing* 7 (IEEE 2002), http://grouper.ieee.org/groups/802/802_tutorials/02-March/IEEE_DSRC_Stds_Tutorial_03-10-02.ppt
(indicating that the 5.9GHz network will be able to transmit data at speeds between 6-27 mbps); *see also Internet and TV Offers*, XFINITY, https://www.xfinity.com/learn/offers (indicating that fr $44.99 a month, you can get 25 mbps of broadband capability).

[67] *See generally Legal Environment for Driverless Vehicles*, *supra* note 6, at 24–27 (discussing the types of information that CVs with DSRC hardware may be able to collect and transmit, and the possible security ramifications of the transmittal of this broad a range of information).

[68] *See Connected Vehicle Challenges*, *supra* note 10 (explaining the technological abilities of dedicated short-range communications).

A CV's relatively limitless ability to transmit the information it collects raises more privacy challenges when the format of the way it transmits data is taken into account. Rather than data transmissions that take the form of a telephone call, where the person who is being called must accept the call before any message or data can be transmitted, CVs will broadcast the information they collect like a radio—where anybody can tune in.[69] A CV user, therefore, may likely have no ability to discriminate as to who gets to analyze the data their vehicle collects. Whether that be a complete stranger, close family friend, or hated enemy, all entities that have access to the DSRC communications network will have an equal ability to access the information any one CV broadcasts.[70]

With respect to the limitations that exist on the data transmission network that CVs use, the range of CV communication is limited to anywhere between 10 and 1,000 meters,[71] depending on the type of communication that is attempted—CV to CV ("V2V") or CV to sensor embedded in the infrastructure ("V2I").[72] This means that it may not be rare for V2V or V2I data transmissions to fail as a result of "some of the receivers" that communicate with CVs moving out of the transmission range of the CV that is sending that information.[73] And this problem is only exacerbated by the fact that any one information exchange performed by a CV has to be done in a matter of seconds.[74] Moreover, it should be mentioned that the

---

[69] *See* José J. Anaya et al., *A Novel Geo-Broadcast Algorithm for V2V Communications over WSN*, 3 ELECGJ 521, 522 (2014) (explaining the broadcast features inherent in CV communications); *see also* Bill Howard, *V2V: What are Vehicle-to-Vehicle Communications and How do They Work?*, EXTREMETECH (Feb. 26, 2017), https://www.extremetech.com/extreme/176093-v2v-what-are-vehicle-to-vehicle-communications-and-how-does-it-work/4 (suggesting possible formats in which V2V information can be communicated).

[70] *See Anaya*, *supra* note 69, at 522. (explaining the communication capabiliti es of CVs).

[71] Xiaomin Ma et al., *Performance and Reliability of DSRC Vehicular Safety Communication: A Formal Analysis*, EURASIP J WIREL. COMM 2–3 (2009); *see also Vehicle-to-Vehicle Communications:*
Readiness of V2V Technology for Application 26, NHTSA (Aug. 2014), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf.

[72] *See* Ma, *supra* note 71, at 2 (explaining dedicated short-range communicat ions).

[73] *See id*. at 2–3 (explaining how vehicles mobilities' may adversely affect communications).

[74] *Id.* at 3. A CV only has a matter of seconds to complete any data transmission it initiates because, by definition, the CV will be moving away from the computer with which it is attempting to communicate.

network through which CVs communicate is highly sensitive to the topography around it, and to certain reflective surfaces.[75] These two factors are currently frustrating the CV communications being made in pilot programs throughout the country.[76]

Despite its weaknesses, however, the DSRC network allows for CVs to take part in relatively uninhibited information transmission.[77] No real impediment exists for CVs from transmitting the types of private information they can collect. And, as of today, the CV system is inherently dependent on data transmissions to and from private third parties (V2V communications) and governmental agencies (V2I communications).[78] For these exact reasons, it is imperative that we identify the legal issues that are created by a CV's capability to transmit information it collects, with particular focus on how existing laws and rules may exacerbate privacy issues implicated by widespread CV use. Failing to do so could expose the highly sensitive private information of many Americans to improper use by third parties.

III. LEGAL ISSUES THAT ARE CREATED BY THE DATA TRANSMISSION CAPABILITIES OF CVS, AND HOW EXISTING LAWS AND RULES MAY NOT BE ADEQUATELY PROTECTIVE OR COULD EVEN EXACERBATE THESE ISSUES.

In his seminal work *The Path of the Law*, Oliver Wendell Holmes wrote that "[i]f you want to know the law . . . you must look at it as a bad man, who cares only for the material consequences which such knowledge enables him to predict, not as a good one, who finds his reasons for conduct, whether inside the law or outside of it, in the vaguer sanctions of conscience."[79] In this spirit, analyzing the data transmission capabilities of CVs from the "bad man's" perspective uncovers several data privacy concerns that may be implicated by widespread CV use, all of which will need to be answered before CV technology is fully operationalized.[80] For the

---

[75] *Id.* at 2–3.

[76] *See id*. at 2–3 (for discussion of communication limits for CVs).

[77] *See Readiness of V2V Technology*, *supra* note 71, at 145 (for discussion of safety functionality).

[78] *Id.* at 13.

[79] Oliver Wendell Holmes, Jr., *The Path of the Law*, 10 HARV. L. REV. 457, 459 (1897).

[80] *See Readiness of V2V Technology, supra* note 71, at 144 (for discussion of data privacy issues).

sake of organization, I will address each of these privacy concerns in the context of the differing parties CVs are designed to communicate with: (1) other CVs on the road, (2) state-owned sensors embedded in the infrastructure, and (3) independent commercial businesses.

1. Data Privacy Issues Implicated by V2V Communications.

As has already been mentioned several times, a properly functioning CV scheme requires high levels of information to be transmitted between CVs operating on the road that have no contractual relationship between each other (also known as "V2V communications").[81] This means that CVs are designed to regularly transmit potentially sensitive data to private third parties who are literally "passing them by." From the "bad man's" perspective, this relatively new information swap scheme presents novel opportunities to access and use information that he never had a way to get to. Accordingly, it is imperative to identify the core privacy issues at the heart of V2V data transmissions, in order to limit the future improper use of the data transmitted by CVs. Especially when considering the types of sensitive data CVs may have the ability to collect and transmit,[82] failure to adequately diagnose the privacy issues resulting from large-scale CV use could have serious consequences.

The first, and perhaps most obvious, issue that the CV V2V communication scheme implicates is the question of who owns the data transmitted by a CV. Or, more specifically, whether receipt of data from a passing CV confers ownership of that data on to the receiver. This is an important question to answer, because if the "bad man" in a passing CV is considered the owner of the data transmitted to him by another CV, he would likely have an unlimited ability to use that information. Hardly trivial, this could potentially result in highly sensitive information making its way into the hands of undesirable parties. For example, a husband in a passing CV could receive information about the occupants of the vehicle that belongs to his recently separated wife,[83] or a stalker

---

[81] *See Connected Vehicle Challenges*, *supra* note 10 (for overview of CV technology).

[82] *See* Walker-Smith, *supra* note 5, at 1789 (examining the breadth of information collected by vehicle communications systems).

[83] *See id.* (explaining that CVs may have the ability to collect information regarding the passengers riding in a CV, which in this case may have serious implications on subsequent divorce proceedings).

could receive data regarding the places a potential victim recently visited.

If we look to the treatment of information communicated via email, faxes, and letters as persuasive authority to answer these data ownership questions, it seems quite clear what the answer should be; people who receive e-mails, faxes, and letters are all considered owners of the physical information they receive.[84] However, because a CV owner is unable to decide who receives the information his vehicle transmits,[85] analogies to e-mails, faxes, and letters may be misplaced because participants in those forms of communication choose the recipient of their messages. Similarly, attempting to answer the question of whether information received by a passing CV is now owned by that CV cannot be answered by analogizing to information received via television and radio broadcasts. Although CV data transmissions are more comparable in form to radio broadcasts,[86] neither radio nor television broadcasts are designed to regularly transmit the types of highly sensitive information that CVs are designed to transmit, like an individual's location or his or her biometric data.[87]

Second, putting aside for the moment the question of who owns the data transmitted in V2V communications, it is also unclear what subsequent uses can be made of the information CVs transmit to private third parties.[88] For example, if a mad scientist was the operator of a CV, could he use any information he collects from passing CVs about their occupant's heart rate to use in experiments he is performing? Could the mad scientist sell the data he collected from passing CVs to pharmaceutical companies for them to use in their own experiments? Again, like the questions of data ownership that CV use implicates, there is very little guidance as to how the issue of subsequent use should be resolved through current legal frameworks.[89] Moreover, if these questions

---

[84] *Gesoff v. IIC Indus.*, 902 A.2d 1130, 1139 (Del. Ch. 2006). In the context of email, the receiver of the email is considered the owner of the email and can use it subsequently for whatever purposes, including litigation.

[85] *See* Anaya, *supra* note 69, at 3 (explaining how CVs will transmit information like a radio signal where anybody can tune in).

[86] *Id.*

[87] *See* Walker-Smith, *supra* note 5, at 1783 (explaining that CVs may have the ability to collect information regarding the passengers riding in a CV, or the heart rate of the passengers).

[88] *Id.* (explaining how some third parties limit data access).

[89] *Id.*

are not solved before widespread operationalization of CV technology, we risk allowing highly sensitive private data to be used with impunity by private-third parties.

2. Data Privacy Issues Implicated by V2I Communications.

Slightly different from the privacy issues associated with V2V communications, in communications involving CVs and the state-owned sensors embedded in the transportation infrastructure (also known as "V2I communications"), the party at the center of potential privacy concerns is not a random "bad man," but rather the state. However, just because V2I communications do not involve information swaps with "unknown" parties, the potential privacy issues that are implicated are no less serious.

For example, with respect to the issues of data ownership and subsequent use touched on above in the context of V2V communications, these concerns are perhaps even more severe in the context of V2I communications. Illustrative of this point is the concern that the state may be required to make any information it collects as a result of CV communications[90] available to the public at large because doing so would be required by state open records legislation.[91]

Each of the states in the U.S. has an open records act that generally applies to all information collected by state governmental bodies in the course of their "official business."[92] Even though information "considered to be confidential by law, either [by] constitutional, statutory, or judicial decision"[93] is generally exempted from production under freedom of information statutes, because of its novelty, few protections exist for the types of information that CVs can collect.[94] For example, in a state like Texas, state agencies are required to make all information available to the public that is "created by, transmitted to, received by, or maintained by an officer . . . or entity performing official business or a governmental function on behalf of a governmental

---

[90] Information it is therefore deemed to have ownership over.

[91] *See, e.g.*, TEX. GOV'T CODE ANN. § 552.002 (West, Westlaw through 85th Legis. Sess. 2017) (outlining an example of one such open records statue, which requires state agencies to make information collected by the agency available to the public).

[92] *See e.g., id.*

[93] TEX. GOV'T CODE ANN. § 552.001 (West, Westlaw through 85th Legis. Sess. 2017).

[94] *See* TEX. § 552.002, *supra* note 91 (explaining how a particular statute would classify V2I data as public information).

body."[95] Information transmitted through V2I communications would likely fall under this state disclosure requirement.

Therefore, it is plausible that states would be required to disclose certain personal information under open records act obligations because that information was recorded by CVs and transferred to the state via V2I communications. And, unlike V2V communications, where the random "bad man" may momentarily receive private information because he or she happens to be within a CV's data transmission range,[96] state disclosure of information collected by CVs as a result of open records acts would allow the public a longer period of access to the information.[97] Whether that be a voice sample, passenger manifest, or operator blood pressure information,[98] this "worst-case scenario" would allow virtually any individual eligible to make an open records request sustained access to highly sensitive private information.[99]

Even if we ignore the issue of a possible obligation on the states to produce data collected from CV communications, the lack of parameters on state agencies for the subsequent use of data collected from V2I communications is also concerning. In fact, some have already articulated concern over the ways state agencies may use information collected by CVs to advance state interests.[100] These concerning uses range from tracking a CV owner's driving patterns—ticketing those who consistently cause traffic jams because of aggressive driving, closely monitoring all CV owners that have criminal histories and who they are associating with, or using each sensor embedded in the transportation infrastructure as a radar gun—ticketing those individuals going too fast.[101] Hardly a trivial use, many would vehemently object to CV data being utilized in this way as an infringement on individual rights to private association[102] and as

---

[95] *Id.*

[96] *See* Ma, *supra* note 71. CVs have data transmission range between 10 and 1,000 meters.

[97] *See, e.g.*, TEX. GOV'T CODE ANN. § 552.006 (West, Westlaw through 85th Legis. Sess. 2017) (providing an example of an open records statute that could subject CV data to public disclosure).

[98] *See* Walker-Smith, *supra* note 5, at 1783 (for types of data that CVs can collect).

[99] *See, e.g.*, § 552.002, *supra* note 91 (for an example of an open records statute requiring a state agency to make information it gathers available to the public).

[100] *See* Devlin, *supra* note 34 (discussing various uses the state may have for information taken from autonomous vehicles).

[101] *Id.*

[102] *See NAACP v. Ala. ex rel. Patterson*, 357 U.S. 449 (1958) (for a general

a breach of one's rights to be free from unreasonable searches and seizures.[103]

3. Data Privacy Issues Implicated by Communications between CVs and Independent Commercial Businesses.

Finally, although independent commercial businesses are currently unable to access the DSRC network through which the CV system operates, because of the significant congressional pressure to change this policy,[104] it is worth discussing the potential privacy issues that CV-commercial business data transmissions implicate. Moreover, when considering the relatively rapid pace at which industry tends to operationalize new technology, the privacy issues created by CV–commercial business data transmissions are likely to be the first types of privacy problems created by the introduction of CV technology that we encounter in the real world.[105]

Already a common practice, the harvesting of private data about consumers by commercial businesses has become so usual that consumers no longer seem to care.[106] In fact, businesses like Yahoo are in the process of patenting "spying billboards" that collect biometric data on passersbys, like their demography or whether their eyes are focusing on the billboard in order to provide more targeted ad information.[107] With this background knowledge, it may seem unlikely that any new legal protests would be made if a

discussion on the right to privately associate).

[103] *See Katz v. United States*, 389 U.S. 347 (1967) (discussing reasonable expectations of privacy a person can have while talking in a phone booth, with respect to the Fourth Amendment right against unreasonable searches and seizures).

[104] *See Legal Environment for Driverless Vehicles*, *supra* note 6, at 24 ("The FCC is under Congressional pressure to re-allocate parts of the now-dedicated [communications] spectrum" that CVs currently use to communicate "to other types of wireless users," which includes commercial businesses).

[105] *See id.* (discussing the pressure by Congress to allow CVs to communicate with non-CV devices).

[106] *See* Walker-Smith, *supra* note 5, at 1783 (discussing data that companies compile about their customers); *see also* Steven Rosenbush & Michael Totty, *How Big Data Is Changing the Whole Equation for Business,* WALL STREET JOURNAL (Mar. 10, 2013), https://www.wsj.com/articles/SB10001424127887324178904578340071261396666 (discussing information that companies can track and use for their benefit); *see also* SOCIAL NETWORKING: LAW, RIGHTS, AND POLICY 308 (Paul Lambert ed. 2014) (illustrating that, at the end of a normal day, the author of the book had over 150 sites tracking his personal information).

[107] Ilyse Liffreing, *Yahoo's "Smart" Billboard Takes Outdoor Data-Collection to the Next Level*, CAMPAIGN (Oct. 14, 2016), http://www.campaignlive.co.uk/article/yahoos-smart-billboard-takes-outdoor-data-collection-next-level/1412220.

commercial business, say Jiffy Lube, erected its own CV sensors on state highways around the country in order to collect information about the integrity of CV equipment driving on the road. However, as has been mentioned earlier, because of the type of data that CVs are able to collect and the way that CVs transmit that data, potential data transmissions between commercial businesses and CVs create privacy issues that do not appear in typical commercial business data collections.[108]

For example, unlike the typical way that businesses collect data on consumers—tracking customer purchases, asking potential consumers to fill out questionnaires, or recording clicks a consumer makes on a retailer's website[109]—operators of CVs are not able to softly guide what businesses collect information on them by deciding what sites not to visit or what stores not to purchase products from.[110] This is because CV transmissions are akin to radio signals—where anybody can tune in.[111] Moreover, the type of intimate data that can be transmitted over a CV communication—biometric data, or passenger manifest data[112]—is rarely tracked through typical business data collection practices.[113] Therefore, CV communications enable commercial businesses to collect new types of private information that they never had access to, about customers that they may have never been able to collect information about before.

The new reams of information that commercial businesses may gain by getting access to the CV data communication network is concerning when considering that commercial businesses are likely to be "free riders" on the CV communication network, merely collecting information transmitted by CVs and not themselves transmitting information intended to advance the transportation

---

[108] *See* Devlin, *supra* note 34 (discussing various types of information taken from autonomous vehicles); *see also Legal Environment for Driverless Vehicles*, *supra* note 6, at 24 (discussing how autonomous vehicles transmit information to other vehicles and companies).

[109] *See* Steve Kroft, *The Data Brokers: Selling Your Personal Information*, 60 MINUTES (Mar. 9 2014), http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ (discussing methods companies have for obtaining personal information).

[110] *See id.* (discussing how the websites people choose to visit can track their information).

[111] Anaya, *supra* note 69, at 522.

[112] Walker-Smith, *supra* note 5, at 1783.

[113] *See id.* (indicating the use of cookies, fingerprint scanners, infrared cameras, and other digital tools to collect the type of intimate customer data that can be transmitted on the CV communication network).

goals of the CV system.[114] This lack of a *quid pro quo* relationship that usually exists in business data collection[115] may cause consumers to finally become fed up with the significant amount of private information commercial businesses would be able to collect about them if given access to the CV communication network. Understandably, CV operators may feel like it would be unfair for commercial businesses to collect so much information about them without getting anything in return.

Putting aside these concerns for the moment, like in the case of V2V and V2I communications, it is also necessary to determine what fair uses commercial businesses should be able to make of private information received from CVs. And more specifically, to what extent private commercial businesses should be allowed to co-opt the CV transportation network in providing data for their business. For example, could a private investigation business place CV sensors around the country precisely in order to collect as much information on all individuals as possible in order to facilitate any future investigation? Or could a pharmaceutical company place CV sensors around the country in order to track the heart rates of CV operators in order to bolster their medical studies? As is touched upon in some of the Department of Transportation's factsheets regarding the CV pilot program, part of the CV pilot program's success is attributed to the low latency of the network through which CVs communicate.[116] Should businesses then be allowed to co-opt the CV transportation network, slowing CV operations, all in the name of advancing their own private business goals?

IV. STATE LAWS THAT ATTEMPT TO GRAPPLE WITH THE PRIVACY ISSUES IMPLICATED BY WIDESPREAD CV USE, AND THEIR INABILITY TO DO SO COMPLETELY.

Perhaps unsurprising, state laws regarding the protection of private data are ill-equipped to tackle the numerous privacy issues

---

[114] *See Connected Vehicle Challenges*, *supra* note 10 (explaining that unlicensed interference could negatively impact the intended functions of the CV data communication network).

[115] *See* Adam Thierer, *Relax and Learn to Love Big Data*, U.S. NEWS & WORLD REPORT (Sept. 16, 2013), https://www.usnews.com/opinion/blogs/economic-intelligence/2013/09/16/big-data-collection-has-many-benefits-for-internet-users (explaining that businesses usually collect data on consumers, but the consumers usually benefit from enhanced services).

[116] *See Connected Vehicle Challenges*, *supra* note 10 (explaining that low latency provides for speedy message transmission and delivery assurance).

that pervasive implementation of CV technology could create.[117] In large part, this seems to be a result of the relative newness of CV technology, the lack of awareness concerning the potential of CVs to transmit highly sensitive information to private third parties, and the failure of existing state laws to anticipate the kinds of information CVs could allow government agencies to collect.[118] Ironically, this inadequacy is even exacerbated by open records laws intended to obtain more effective government[119]—perhaps suggesting that, as written, state laws regarding the protection of private data make us worse off rather than better.

To illustrate this point, I will identify how current state laws concerning (1) data breaches, (2) disclosure of information pertaining to motor vehicles, and (3) laws regulating the "event data recorders" installed in cars fail to respond to the key privacy concerns at the heart of CV operation. Because of the large number of state laws and regulations that could potentially govern data privacy issues, however, this section should not be considered a complete exploration of how current state law is largely inadequate in answering the privacy issues created by CV operation, but rather merely an explanation of how the legislation that would be most likely to solve the privacy issues created by CVs fails in this regard.

1. State Data Breach Laws

Beginning around 2002, "[f]orty-eight states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands . . . enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving

---

[117] *See* GRETCHEN RAMOS, AUTONOMOUS VEHICLES: WILL THE CYBERSECURITY RISKS BE ADDRESSED?, (Bloomberg BNA, 15 PVLR 1932, 2016) (explaining that "there are currently no state laws in place addressing the security and privacy issues . . . associated with the collection, use, and storage of data stemming from autonomous vehicle use.").

[118] *See* Ellen P. Goodman, *Self-driving Cars: Overlooking Data Privacy is a Car Crash Waiting to Happen*, THE GUARDIAN (June 8, 2016), https://www.theguardian.com/technology/2016/jun/08/self-driving-car-legislation-drones-data-security (explaining that current state data laws fail to acknowledge the data security and privacy aspects associated with the kinds of information CVs can collect and use).

[119] *See Open Records Laws and Resources*, JUDICIAL WATCH, http://www.judicialwatch.org/open-records-laws-and-resources/ (explaining that open records laws generally inhibit government corruption, but allow public access to government documents and information).

personally identifiable information."[120] Commonly nicknamed "data breach laws," the purpose of these laws was to place a duty to inform on both governmental and non-governmental agencies that deal with sensitive information whenever the integrity of that information was compromised.[121] Although versions of these laws vary slightly from state to state, data breach laws provide few protections from the privacy concerns implicated by the information swaps inherent in the CV scheme. Chiefly, this seems to be because of the failure of data breach laws to envision the way in which CVs are designed to exchange sensitive information.

For example, as can be seen in the data breach law enacted by Alaska's state legislature,[122] state data breach laws ignore the issue of when someone is considered an "owner" of data. Specifically, data breach laws take for granted the idea that a clear owner for private data exists.[123] This assumption makes the application of state data breach laws to the CV scheme problematic, because as was touched on above, the question of who owns the data collected from a CV is not entirely clear. Because CVs transmit data in a format similar to radio broadcasts,[124] many people may be able to attain private information transmitted by a CV who are not necessarily the intended recipients of that information. Should those people then be considered owners of that information? If they are considered owners of that private information, then state data breach laws would provide no protections for private citizens whose sensitive information was compromised through the CV communication scheme.[125]

Additionally, data breach laws are unlikely to provide protections for the private information belonging to CV operators

---

[120] *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. The two states without such a law are Alabama and South Dakota.

[121] *See, e.g.*, MICH. COMP. LAWS § 445.63, 445.72 (West, Westlaw through 99th Legis. Reg. Sess. 2017) (for an example of one of these state laws).

[122] ALASKA STAT. § 45.48.010 (West, Westlaw through 30th Legis. Reg. Sess. 2017).

[123] *See id*. "If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach."

[124] Anaya, *supra* note 69, at 522.

[125] *See* ALASKA § 45.48.010, *supra* note 122. Disclosure obligations imposed by the law would be obsolete if there is no breach.

because data breach laws only place affirmative duties to notify when private data has been accessed without authorization.[126] Like the failure of data breach laws to explicitly deal with the question of data ownership, this also prevents the neat application of state data breach laws to the CV context because the question of who has authorization to access information transmitted by a CV is often difficult to answer.[127] As was mentioned above, CVs broadcast the information they have collected like a radio—where anybody can tune in. Considering this format of information transmission, could any person within broadcast be considered an "authorized" recipient of that information? If so, then data breach laws would not likely apply to CV communications.

Lastly, data breach laws are unlikely to adequately respond to the privacy concerns implicated by CV operation because of how these laws define what is considered private information.[128] Specifically, some data breach laws define "personal information" as merely someone's "Social Security number," "driver's license number," or "financial account number."[129] Therefore, almost all of the types of data that CVs can transmit—biometric data, car occupancy data, or driver personality data—would not fall under the category of personal information as defined by these laws. Accordingly, state data breach laws would fail to prevent the transmission of the most "private" types of data that a CV is likely to be able to collect.

2. Motor Vehicle Disclosure Acts

Inspired by the Federal Driver's Privacy Protection Act,[130] most states have enacted legislation limiting the types of personal information contained within motor vehicle records that state

---

[126] *See, e.g.*, TEX. BUS. & COM. CODE § 521.053 (West, Westlaw through 85th Legis. 2017) ("'breach of system security' means *unauthorized* acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person . . . ") (emphasis added).

[127] *See* KAN. STAT. § 50-7a01 (West, Westlaw through Legis. Reg. Sess. 2017) (depicting the impossibility of current state data breach laws to protect against the transmission of data that passes through the CV communication scheme).

[128] *See* Reid J. Schar & Kathleen W. Gibbons, *Complicated Compliance: State Data Breach Notification Laws*, BLOOMBERG NEWS (Aug. 9, 2013), https://www.bna.com/complicated-compliance-state-data-breach-notification-laws/ (discussing the state laws' varying definitions of "personal information").

[129] KAN. § 50-7a01, *supra* note 127.

[130] UNIFORM MOTOR VEHICLE RECORDS DISCLOSURE ACT, 18 U.S.C. § 2721–2725 (1994).

agencies can disclose.[131] All highly similar to model legislation provided by the American Association of Motor Vehicle Administrators ("AAMVA"),[132] these state acts provide basic protections against the dissemination of "personal information" or "highly restricted personal information"[133] found in motor vehicle records. Although, with small revisions, these acts could significantly reduce public access to sensitive personal information gathered through CV communications, as drafted, they are unlikely to provide any such protections.[134]

For example, although most Motor Vehicle Disclosure Acts expressly forbid the disclosure of "information that identifies an individual, including such individual's photograph or image, Social Security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information,"[135] these acts allow for the disclosure of such personal information when it is related to "matters of motor vehicle or driver safety."[136] However, because the entire CV transportation scheme is characterized by the U.S. Department of Transportation as necessary in order to ensure safe transportation,[137] it seems likely that all information transmitted through the CV communication scheme could be considered to fall under this exception to the general rule against disclosure.[138] If that happens, these Motor Vehicle Disclosure Acts would not prevent the disclosure of any personal information belonging to a CV operator, which would allow private third parties to access that information freely.

Even if the phrase "matters of motor vehicle safety" was interpreted narrowly so as to prevent all information

---

131 *See, e.g.,* CONN. GEN. STAT. ANN. § 14–10 (West, Westlaw through Reg. Sess. 2017); MO. ANN. STAT. § 32.091 (West, Westlaw through 99th G.A. Sess. 2017); TEX. TRANSP. CODE ANN. § 730.002 (West, Westlaw through 85th Legis. Sess. 2017).

132 *Model Legislation Concerning Disclosure of Personal Information Contained in Motor Vehicle Records*, AM. ASSOC. OF MOTOR VEHICLE ADMIN., http://www.aamva.org/uploadedFiles/MainSite/Content/SolutionsBestPractices/BestPracticesModelLegislation(1)/ModelLaw_DisclosurePersnlInfoInMVRecords.pdf.

133 *See* 18 U.S.C. § 2721–2725, *supra* note 130 (laying out the terms of the federal act).

134 *See* 18 U.S.C. § 2725(3), *supra* note 130 (defining "personal information" per the statute).

135 *Id.*; 18 U.S.C. § 2721(a), *supra* note 130.

136 18 U.S.C. § 2721(b), *supra* note 130.

137 *Connected Vehicle Challenges*, *supra* note 10.

138 *See id*. (supporting the idea that all CV communications could fall under the broad statutory definition of "matters of motor vehicle or driver safety").

communicated through the CV scheme from falling under one of the exceptions to the general rule against disclosure, like with the data breach laws, the definition of personal information in these Motor Vehicle Disclosure Acts does not cover each of the types of information a CV can communicate. Specifically, "personal information" in these acts is often defined so as not to prevent the dissemination of information relating to "other contents of a motor vehicle record, including information on vehicular accidents, driving or equipment-related violations, dispositions by any court or administrative body, and driver's license or registration status."[139]

Accordingly, like state data breach laws, state Motor Vehicle Disclosure Acts are unlikely to comprehensively prevent the disclosure of all of the types of sensitive private information that CVs may have the ability to disseminate. As written, Motor Vehicle Disclosure Acts would fail to prevent the dissemination of information like the integrity of a CV's component parts (e.g. whether the actual mechanical parts making up a CV are close to failure), whether a CV was speeding, or conversations that have taken place in a CV.[140] Hardly trivial, some have already begun to cringe at the now very real idea that everyday technologies would capture our most intimate conversations and make those same conversations available to third parties.[141] Imagine, for example, how embarrassing it would be for even a complete stranger to hear a conversation between you and your wife where she tells you her baby is "not yours."[142]

3. Laws Regulating Electronic Device Recorders

Introduced into commercial markets in the early 1990s,[143] event data recorders ("EDRs") are small computers vehicle

---

[139] *Model Legislation*, *supra* note 132, at § 3(h).

[140] *See generally id*. (establishing what model Motor Vehicle Disclosure Acts entail).

[141] Chris Matyszczyk, *Samsung's Warning: Our Smart TVs Record Your Living Room Chatter*, CNET (Feb. 8, 2015), https://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/. Here, one tech writer reacts to Samsung's new voice recording and transmission policy.

[142] *See id*. (hypothesizing such a scenario).

[143] R. Brent Cooper, *Event Data Recorders: Balancing the Benefits and Drawbacks*, IRMI (Aug. 2008), https://www.irmi.com/articles/expert-commentary/event-data-recorders-balancing-the-benefits-and-drawbacks/. "The first such devices were available in the 1970s but were not installed on most passenger cars until 20 years later."

manufacturers began installing in cars to "capture information, such as the speed of a vehicle and the use of a safety belt, in the event of a collision to help understand how the vehicle's systems performed."[144] Often used by law enforcement in order to reconstruct accidents,[145] state legislatures began crafting statues limiting who was allowed to access the information compiled by EDRs after learning that various parties could do so for reasons not pertaining directly to driver safety.[146] Beginning with California in 2004, "[s]eventeen states—Arkansas, California, Colorado, Connecticut, Delaware, Maine, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Oregon, Texas, Utah, Virginia and Washington—[] enacted statutes relating to event data recorders and privacy."[147] Although these state laws directly limit the ability of third parties to access private information collected by motor vehicles, like state data breach laws and state Motor Vehicle Disclosure Acts, as written they provide no protections from the data privacy issues implicated by CV use.[148]

The wording of Utah's EDR law nicely illustrates the inability of these statutes to address the privacy concerns created by CV data transmission capabilities. Specifically, EDR laws make it a crime for "a person who is not the owner of the motor vehicle"[149] to access information collected by a motor vehicle's EDR. But, rather than defining the term "event data recorder" broadly to mean any computer on a vehicle that collects information about any event that a vehicle experienced, "event data recorder" is defined narrowly as "a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (e.g., vehicle speed vs. time) or during a crash

---

144 *Privacy of Data From Event Data Recorders: State Statutes*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

145 Martin Kaste, *Yes, Your New Car Has A 'Black Box.' Where's The Off Switch?* NPR (Mar. 20, 2013), http://www.npr.org/sections/alltechconsidered/2013/03/20/174827589/yes-your-new-car-has-a-black-box-wheres-the-off-switch.

146 *See* Cooper, *supra* note 143 (listing states that have passed EDR regulations).

147 *Privacy of Data*, *supra* note 144; *see also* N.D. CENT. CODE ANN. § 51-07-28 (West, Westlaw through 65th Legis. Reg. Sess. 2017) (providing an example from North Dakota of one state statute).

148 *See generally Model Legislation, supra* note 132 (offering an example of privacy legislation regarding motor vehicle records).

149 UTAH CODE § 41-1a-1503(1)(iii) (West, Westlaw through General Sess. 2017).

event (e.g., delta-V vs. time), intended for retrieval after the crash event."[150] This definition of EDR narrows the scope of EDR laws to the point of preventing their application against "bad-men" who may want to access the sensitive information CVs will have the ability to collect, but that cannot reasonably be described as "a device or function in a vehicle that records the vehicle's dynamic time-series data."

Even if a court decided to interpret the definition of EDR in EDR laws broadly to the extent that the definition covered all information collection capabilities that CVs may have, often EDR laws have an exception to the general rule against third-party access to information collected by an EDR when that information "is used for the purpose of improving motor vehicle safety."[151] As discussed in the section pertaining to Motor Vehicle Disclosure Acts, it is likely that any information communicated through the CV scheme will be considered as "used for the purpose of improving motor vehicle safety."[152] Therefore, even if interpreted narrowly, EDR laws are unlikely to prevent the communication of information collected by a CV, because all of that information is likely to fall under the exception to the general rule against disclosure of EDR information in EDR laws.[153] Accordingly, EDR laws are unlikely to assuage the privacy concerns implicated by widespread CV. Just like data breach laws and Motor Vehicle Disclosure Acts, EDR laws similarly fail to prevent the dissemination of the various types of private information CVs will be able to communicate.

V. PRELIMINARY SUGGESTIONS FOR HOW EXISTING STATE LAWS COULD BE AMENDED IN ORDER TO GRAPPLE WITH SOME OF THE PRIVACY ISSUES IMPLICATED BY THE CV DATA TRANSMISSION

---

[150] *See, e.g.,* UTAH CODE § 41-1a-1502(2) (West, Westlaw through Gen. Sess. 2017); MONT. CODE ANN. § 61-12-1001(1) (West, Westlaw through Sess. 2017); ORE. REV. STAT. ANN. § 105.925(1) (West, Westlaw through Reg. Sess. Legis. 2017).

[151] *See, e.g.,* N.J. STAT. ANN. § 39:10B-8(a)(3) (West, Westlaw through Legis. Sess. 2017); WASH. REV. CODE ANN. § 46.35.030(1)(c) (West, Westlaw through 3rd Spec. Sess. of Wash. Leg. 2017); CAL. VEH. CODE § 9951(c)(3) (West, Westlaw through Ch. 181 Reg. Sess. 2017).

[152] *See Connected Vehicle Challenges*, *supra* note 10 (describing DOT's characterization of CV communications as essential for the improvement of motor vehicle safety).

[153] *See id.* (indicating DOT's priority on the improvement of motor vehicle safety).

SCHEME.

Considering the novel technological capabilities CVs may have in the near future to collect and send private information, the failure of existing state laws to fully respond to the privacy concerns associated with the implementation of CV technology is unsurprising. However, with slight tweaks, many of these laws could prove valuable to that end. In this section, I will make suggestions for how existing state laws could be amended to better respond to the privacy concerns implicated by CV use. Specifically, these suggestions are (1) updating key language in current state laws impacting disclosures of private information to ensure that they cover the unique aspects of CV data collection and dissemination, (2) placing restrictions on the subsequent use of information obtained through open records acts, and (3) amending data breach laws by placing an affirmative duty on state governments to disclose to CV participants when their personal information is collected by the state and to explain what type of information was collected.

This section should not be seen as a comprehensive list of reforms to state laws impacting the disclosure of private information, but rather an attempt on my part to point out what I think the most effective reforms to current state law could be. As I alluded to in the introduction to this paper, the data collection capabilities of CVs implicate many more privacy issues other than those involving CV communications over the DSRC network. For example, now that CVs are likely to have the ability to collect all sorts of private information about us, we will need to re-analyze the legality of user agreements between car manufacturers and their clientele, which allow the manufacturer almost unlimited access to the information a CV can collect.[154] However, because these issues are largely out of the scope of this paper, I will not attempt to provide tentative solutions for them in this section. Hopefully, future scholarship will carry on this baton.

1. Updating Key Language in Current State Laws Impacting Disclosures of Private Information

Simply put, as written, state privacy laws are unable to provide sufficient protection from the privacy issues that would be created

---

[154] *See Nissan*, *supra* note 42 (stating that, in its user agreement, if Nissan is not given access to the data the car can record, the car will not be able to operate as intended).

by widespread use of CV technology. And, when you consider that analysts expect "over 380 million connected cars will be on the road by 2021,"[155] it is obvious that this is a problem that needs to be fixed quickly. However, this does not mean that existing state privacy laws should be scrapped altogether and new more technologically aware laws passed in their place. Rather, amending key terms in these laws may be the cheapest and most convenient way to provide substantial protections from the privacy issues implicated by CV use. In fact, many, if not all of the privacy issues implicated by CV use could be avoided with two amendments to state EDR laws: (1) broadening the definition of "Electronic Recording Device" and (2) limiting the "improvement to motor vehicle safety" exception to the general rule against third-party access to information collected by an EDR.

First and foremost, by simply broadening the definition of "Electronic Recording Device"[156] in state EDR laws to encompass "any device in a motor vehicle that records information about the vehicle or its occupants," state EDR laws could provide sweeping protections from the privacy issues created by CVs. If this amendment were made to the EDR law in Utah for instance, Utah's EDR law would read as follows: "[e]vent data that is recorded on any [device in a motor vehicle that records information about the vehicle or its occupants] . . . may not be retrieved by a person who is not the owner of the motor vehicle."[157]

However, this amendment alone is insufficient to prevent against the privacy issues created by CV use due to the exception to the general rule against third-party access to information collected by an EDR that exists in current EDR laws. Specifically, as has been mentioned above, this exception allows for the disclosure of any information collected by an EDR that is intended to "improve[] motor vehicle safety."[158] Since the purpose of the CV communication scheme is to facilitate safe transportation, read

---

[155] John Greenough, *The Connected Car Report: Forecasts, Competing Technologies, and Leading Manufacturers*, BUSINESS INSIDER (Jun. 10, 2016), http://www.businessinsider.com/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3.

[156] *See* UTAH § 41-1a-1502, *supra* note 150, at (2) (*citing* 49 C.F.R. § 563.5, which defines EDR as "a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (e.g., vehicle speed vs. time) or during a crash event (e.g., delta-V vs. time), intended for retrieval after the crash event.").

[157] *See* UTAH § 41-1a-1503, *supra* note 149, at (2) (quoting the statute and adding in proposed amendment).

[158] *Id*. at § 41-1a-1503(4)(d).

broadly, this exception may be used to justify third-party access to any information collected by a CV.[159] Therefore, it will also be necessary to clarify that CV communications to private third parties do not fall under this exception in order for any proposed amendments to state EDR laws to have maximum effect.

If completed, making these changes could significantly reduce private third-party access to the information a CV could collect and disseminate. For instance, effectuating this proposed change to state EDR laws would prevent practices like neighbors placing sensors outside of their house so that they can collect the data disseminated from your CV, or ex-husbands stalking their ex-wives in the hopes of facilitating a data exchange with their CV. CV operators would no longer have to worry that the information their CV transmits about them would be collected by private third parties without their consent.

Likewise, (1) broadening the definition of "personal information"[160] in state Motor Vehicle Disclosure Acts to encompass the new types of personal information that CVs can collect and (2) limiting the "matters of motor vehicle or driver safety"[161] exception to the general rule against third-party access to motor vehicle record information would also provide substantial protections from the privacy issues created by CV use.

If the definition of "personal information" in the model State Motor Vehicle Disclosure Act was modified to "any information collected about a person, or his or her motor vehicle," for example, the act would read as follows: "the department, and any officer, employee, agent or contractor thereof shall not disclose [any information collected about a person, or his or her motor vehicle] obtained by the department in connection with a motor vehicle record."[162] Like with EDR laws, however, this legislative amendment would also need to be done simultaneously with an

---

159 *See Connected Vehicle Challenges, supra* note 10 (explaining also how connected vehicles contribute to driver safety).

160 *See Model Legislation*, *supra* note 132, at § 3(h) (for a current definition of "personal information" in Motor Vehicle Disclosure Acts).

161 *See id.* at § 5. Although Motor Vehicle Disclosure Act laws generally prevent third parties from being able to access a person's motor vehicle records, an exception arises if that third party wants to access information about a person's motor vehicle records "in connection with matters of motor vehicle or driver safety." Read broadly, because the purpose of the CV communication scheme is to facilitate safe transportation, this exception could be used to justify third-party access to any information about a person appearing in their motor vehicle records.

162 *Id.* at § 4. The author adds proposed amendment language.

amendment to one of the exceptions to the general rule against third-party access to motor vehicle record information in order to have maximum effect. Specifically, an amendment would need to be made clarifying that CV communications do not qualify under the "matters of motor vehicle or driver safety"[163] exception to the general rule against third-party access to a person's motor vehicle records.

If completed, these two amendments could significantly reduce third-party access to information collected by a CV through open records requests. For instance, this proposed change to Motor Vehicle Disclosure Act laws would prevent the same snooping neighbors or ex-husbands above from obtaining any sensitive information about you from your CV through open records requests, rather than through first-hand data transmissions. Considering that it would probably be easier for our resident "bad man" to make an open records request rather than to physically follow around persons whose private information he would like to access, functionally, this amendment may even provide more protections against third parties from accessing private sensitive information.

Although it may seem like broadly amending state EDR and Motor Vehicle Disclosure Acts in these ways could prevent public access to valuable information collected by CVs on the road, this concern is largely overblown. This is because, as written, these laws provide several exceptions to the general rule against disclosure of private information to third parties when the information deals with matters of public concern like "motor vehicle emissions, motor vehicle product alterations,"[164] or "security communications."[165] So, for example, if a CV was involved in a crash on the road, existing exceptions to EDR laws would allow the broadcast of any distress information to state agencies or privately contracted emergency response firms.[166] Therefore, these proposed amendments could be effectuated without substantively affecting access to the types of public safety information that CVs can collect.

---

163 *See id.* at § 5 (laying out the exception).

164 *See id*. (laying out the exception).

165 *See* UTAH § 41-1a-1503, *supra* note 149, at (2)(f) (West, Westlaw through General Sess. 2017) (establishing that data may be retrieved in particular emergency situations).

166 *See id*. (laying out that data could be retrieved in case of an emergency medical situation).

2. Placing Restrictions on the Subsequent use of Information Obtained through Open Records Acts.

Although amending key terms in current state laws governing the disclosure of private information significantly reduces the privacy concerns associated with CV use, there are also some instances in which adding new provisions to existing state laws provides robust protections against the privacy issues created by CVs.[167] The question of what subsequent uses can be made of the information obtained through state open records acts is a good example of this.[168]

As written, state open records acts compel state agencies to make all information available to the public that is "created by, transmitted to, received by, or maintained by an officer . . . or entity performing official business or a governmental function on behalf of a governmental body."[169] Previously mentioned before, this could potentially allow private third parties access to any of the sensitive personal information a CV may transmit to state agencies through V2I communications. If that were to happen, state open records acts do not currently provide any limits as to the ways that third party could subsequently use the information it receives through an open records request.[170] And if that third-party were our resident "bad man," one can only imagine the number of improper uses that could be made of such information.[171]

However, because of the overwhelming governmental oversight benefits that open records act legislation provides,[172] simply preventing the application of state open records acts to the CV data transmission scheme by narrowing the definitions of the act's

---

[167] *See Model Legislation*, *supra* note 132 (for model uniform legislation).

[168] *See supra* Part III for discussion of subsequent uses.

[169] *See, e.g.*, TEX. § 552.002, *supra* note 91, at (a-1).

[170] *See, e.g.*, TEX. § 552.001, *supra* note 93 (illustrating state open records acts in general and that there is no limit on a third party's subsequent use of information received through an open records act request).

[171] *See supra* Part III for discussion of how a bad man may improperly use personal information obtained via V2I communications.

[172] *See, e.g.*, TEX. § 552.001, *supra* note 93 ("The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may retain control over the instruments they have created. The provisions of this chapter shall be liberally construed to implement this policy."); *see also Sunshine Week:The Importance of Public Access to Records*, THE TELEGRAPH (Mar. 14, 2015), http://www.macon.com/news/local /article30220611.html (for general discussion of open records laws).

terms seems inappropriate. For instance, how could citizens adequately police the broad data collection powers CVs may give governments without having unfettered access to details about the types of information the government can collect, and how it collects that information. Moreover, it seems hard to argue that the public does not have a right to access the more "public" types of data—like motor vehicle emissions—that CVs are likely to have the ability to collect.

Therefore, at least one possible solution to the issue of "subsequent use" would seem to be the placement of statutory limits as to how third parties may use information obtained through open records acts. As can be imagined though, choosing these limits is a hard thing to do. If the limits are too broad, many potentially controversial uses of personal information could still be allowed, and if the limits are too narrow, we risk damaging the benefits of governmental oversight that open records acts are meant to provide.

Since the primary purpose of open records laws are to provide transparency as to government operations,[173] I propose that provisions should be added to state open records acts limiting the subsequent use of information received to those activities directly related to the achievement of government transparency. Specifically, these subsequent uses would be the publishing of articles meant to inform the public of government information collection capabilities, using the information to better understand the government's CV data transmission scheme, and the use of information obtained through the open records act process to facilitate future legislative amendments. In order to better police these limitations on subsequent use, parties requesting access to open records act information collected from CV communications would be required to specify how they plan to use the information they requested before they are allowed to receive it.

Although these proposed amendments to existing open records act legislation admittedly create issues both with respect to ex-post enforcement and ex-ante restrictions on releasing data, I think they represent the necessary first-step in what will be a long process to determine what subsequent uses should be made of information collected by CVs. Perhaps CV communications are

---

[173] *See* TEX. § 552.001, *supra* note 93 ("[I]t is the policy of this state that each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees.").

excluded from open records requests altogether and we elect an ombudsman to oversee the government's data collection powers. Or, perhaps we allow the courts to determine category by category what types of information a CV collects should be requestable through the open records act system. There is no simple answer.

But, failing to draw a line somewhere could have extreme consequences. With respect to limiting the subsequent uses of information obtained through open records requests, the burden that would fall on courts or administrative bodies to enforce this proposed amendment is, in my view, insignificant when compared to the consequences of either (1) giving the CV scheme complete immunity from open records requests, or (2) not placing any restrictions on the subsequent use of information received through open records requests.

3. Amending Data Breach Laws by Placing an Affirmative Duty on State governments to Disclose to CV Participants when their Personal Information is Collected by the State, and to Explain what type of Information was Collected.

As written, state data breach laws require both governmental and non-governmental agencies that deal with certain sensitive information to inform the owners of that information whenever its integrity is compromised.[174] Although these laws are largely inapplicable to the CV data transmission scheme because of the way they define "breach" and "personal information,"[175] amending state data breach laws so as to guarantee their application to any transmission of personal information by CV participants to the state may provide the hardiest protections against the data privacy issues created by CV use.

Specifically, by modifying the definition of "breach" in state data breach laws to include "all communications of information by CV participants to state agencies," state data breach laws would read:

---

[174] *See, e.g.*, MICH. § 445.72, *supra* note 121 (providing an example of one state's data breach law).

[175] *See Self-driving Cars, supra* note 118 (discussing the disconnect between data breach laws, privacy laws, and CVs and how some states have addressed CVs in their legal system). In summary, data breach laws as written are largely inapplicable to the CV data transmission scheme because they do not anticipate the types of information a CV could collect, and do not include those types of information in discussions of types of information the acts cover. Because CVs transmit information like a radio, where anybody can tune in, a party who receives information from a CV can hardly be said to have "breached" the CV's security.

"If [the State] owns or licenses personal information in any form that includes personal information on a state resident, and [any of that information was communicated to the state by a CV] . . . [the state] shall, after discovering or being notified of the [CV communication], disclose the [communication] to each state resident whose personal information was subject to the breach."[176]

Highly meaningful, this change could be used to create an affirmative obligation on the part of the state government to inform all CV participants when their personal information is collected by the state, and what kind of personal information was collected at that time. This would mean that whenever the state collects personal information about a CV occupant through V2I communications, it would then be required to notify that CV operator by physical or electronic communication when and what kind of personal information was collected.[177] Because of the sheer volume of CV communications that are likely to trigger this requirement, it is likely that state communications to CV owners may have to be over a state owned and operated database—perhaps similar to the ones that currently manage state toll roads.[178]

When considering the limitless types of data that CVs will be able to collect, and therefore that the state may have access to,[179] these data disclosure requirements may prove helpful in limiting the government from abusing its data collection powers. The thought being that the state would be less likely to operationalize questionable uses of data it collects when it knows countless CV operators will be looking over its shoulder. Moreover, in a time where data security concerns are at an all-time high,[180] by constantly informing a CV operator of the types of information

---

176 *See* ALASKA § 45.48.010, *supra* note 122, at (a) (adding proposed language to one state's statute).

177 *See id.* (again emphasizing the importance of a possible amendment to one state's statute).

178 *See e.g.*, *My TxTag Account*, TXTAG, https://www.txtag.org/vector/account/home/accountLogin.do?locale=en_US&from=Home (providing, as an example, one state's electronic toll collection system). After plugging in certain identifiable information, all toll fees attached to your car are itemized.

179 *See* Walker-Smith, *supra* note 5, at 1783 (discussing technological advancements in data-tracking and sharing).

180 *See* Lorenzo Franceschi-Bicchierai, *Famous iPhone Hacker 'Geohot' Shows Us How Easy It Is To Hack a Computer*, VICE (July 13, 2016), https://motherboard.vice.com/en_us/article/famous-iphone-hacker-geohot-shows-us-how-easy-it-is-to-hack-a-computer (illustrative of data privacy concerns today, as many feel that online information is unsecure).

being collected about him or her, the state could garner much needed public support for the CV program.

As has been explained above, the CV scheme is inherently dependent on high user participation. Therefore, the usefulness of an amendment that could ultimately have the effect of increasing public confidence in the CV program altogether cannot be understated. And, although such an amendment may ultimately be difficult to operationalize, the privacy consequences of not doing so suggest that such an amendment is worth the administrative trouble it may cause. Everyday, cities, counties, and states notify us of when we are taxed—why shouldn't they be required to notify us when they are taking our information, rather than our money, to use in a public program?

CONCLUSION

Imagining the ways in which CVs could positively impact our lives is exciting and easy to do: parents may no longer have to worry about their kids getting into a car crashes on prom night, long morning commutes to work wouldn't get in the way of a last second assignment, and people may not even need to bother with the hassle of owning cars at all—preferring instead to call driverless ubers as needed. But these safety, efficiency, and convenience advantages may come at cost.

Like with many technological innovations, widespread operationalization of CVs could lead to significant breaches in personal privacy that prompt us to reconsider what an added convenience in our lives is worth. CVs are already collecting and sharing information about the speed at which we travel, where we travel, and the traffic signals we use,[181] and experts believe that CVs will only become more intrusive in this respect. Some even speculate that, in time, CVs will be designed to collect and share information about our heart rate,[182] who we drive with,[183] and how we like to drive.[184]

Unless we adapt our existing legislative framework accordingly to account for the novel technological capability CVs may have to collect and disseminate highly sensitive private information, we

---

[181] *Research Data Exchange*, *supra* note 29.

[182] *See* Walker-Smith, *supra* note 5, at 1783 (discussing third-party tracking of one's heart rate).

[183] *See Legal Environment for Driverless Vehicles*, *supra* note 6, at 20 (speculati ng about the evolution of driverless vehicles and data tracking).

[184] *Id.*

risk allowing CVs to explore these limits almost entirely unregulated. Perhaps difficult to envision now, this could lead to highly undesirable scenarios, like scientists utilizing your biometric data without your consent,[185] or your recently separated partner receiving information about who you have had in your car.[186]

It is for precisely these reasons that we must investigate the data privacy issues implicated by widespread CV use and identify where amendments to our existing legal framework will be most effective in curbing the Pandora's box of issues CV technology could usher in. All is not nearly lost, and directed prophylactic measures now could provide robust protections from the privacy issues implicated by CV technology. Certitude in the positive benefits of a technological innovation like CVs should not blind us to the potential problems it may create. As Oliver Wendell Holmes once wrote, "[w]e have been cocksure of many things that were not so."[187]

---

185 *See supra* Part III for discussion of privacy issues implicated by CVs.
186 *See supra* note 83 for cheating spouse example.
187 Oliver Wendell Holmes Jr., *Natural Law*, 32 HARV. L. REV. 40, 40 (1918).