Fast Cars, Open Highways, and Bulk Data Collection: Fourth Amendment Limits on Police Use of Smart Infrastructure

Thomas McAuley[*]

What's more American than cars, highways, and bulk data collection? While not a natural combination, it is quickly becoming a real one. Smart cities are developing smart infrastructure. The simple addition of wireless transceivers to traffic lights, road signs, and highway overpasses enables vehicle-to-infrastructure (V2I) communications. Suddenly, a crosswalk can alert you to a pedestrian. A traffic light can tell you to brake when another driver is running a red light. An interstate exit can warn a trucker about a wrong-way driver. This technology has enormous potential to improve traffic safety.

But these same communications also open the door to a potentially massive area of surveillance. Can the same traffic signal ticket you for running a red light? Can police recreate a suspect's trip using data from a bridge near the crime scene? And when public roadways can sense who is traveling on them, is anonymity in public still possible?

This Note considers whether the Fourth Amendment limits the government's collection and use of V2I communications. Part I gives background on the concept and promise of V2I communications (What is it?). Part I also explains the technology involved and precisely what information is communicated (How does it work?). Part II discusses why law enforcement will want this data despite claims that it is anonymous (How can police use it?). Part II supplements this qualitative discussion with a quantitative demonstration of the associated privacy risks using V2I pilot data and data science techniques. Part III applies the Fourth Amendment to V2I communication (Is it a search? Is it reasonable?). This Note then concludes by discussing considerations for the future of V2I development (What's next?).

* J.D. Candidate, Class of 2025, The University of Texas School of Law. Thank you to Dr. Anna R.W. McAuley and Professor Adam I. Klein for their support.

Introduction

Traffic lights today are not just signals—they are sensors, too. "Smart" infrastructure is quickly but quietly lining public roads. Forty percent of

American intersections will be smart by 2040.[1] This digitization would happen sooner if traffic authorities were not simultaneously connecting the crosswalks, tunnels, bridges, and overpasses stitching those intersections together.

This is the future of the smart city. Vehicle-to-infrastructure (V2I) systems will alert your car to wrong-way drivers on blind turns, pedestrians in crosswalks, and red-light runners. An ambulance will rely on V2I data to clear traffic along the route to the hospital. Traffic engineers will analyze their data to better design road networks. The result will be a new era of intelligent transportation systems characterized by efficiency and safety.

But will it also be marked by constant police surveillance? The same governments responsible for traffic safety are also responsible for law enforcement. Criminal investigators can already reconstruct individual vehicle trips using the data exchanged in V2I deployments across the country.[2] Given the impending proliferation of these systems, the privacy implications of smart infrastructure dwarf those of the plate readers and traffic cameras that investigators use today.

Drivers concerned about their privacy on this future roadway should not look to the Fourth Amendment for protection. This Note explains why the Fourth Amendment does *not* prohibit police collection and use of V2I communications.[3] Part I gives background on the concept and promise of V2I communications (What is it?). It also explains technology involved and precisely what information is communicated (How does it work?). Part II discusses why law enforcement will want this data despite claims that it is anonymous (How can police use it?). Part III applies the Fourth Amendment to V2I communication (Is it a search? Is it reasonable?). This Note then concludes by discussing considerations for the future of V2I development (What's next?).

I. Smart Infrastructure Will Improve Traffic Safety and Congestion

A. Transportation Agencies Are Building Smart Infrastructure to Improve Road Safety

If you bought your car after 2015, it collects and transmits reams of your data. That is because ninety-five percent of the vehicles sold today are

1. Saeed Asadi Bagloee, Madjid Tavana, Mohsen Asadi & Tracey Oliver, *Autonomous Vehicles: Challenges, Opportunities, and Future Implications for Transportation Policies*, 24 J. MOD. TRANSP. 284, 285 (2016).

2. For an analysis of V2I pilot data related to claims of anonymity, see *infra* Part II.

3. This Note does not address the lawfulness of intercepting V2I communications. As discussed in subpart II(B), these communications are broadcasted without encryption. This theoretically allows anyone, including law enforcement, to intercept and read V2I messages. The lawfulness of V2I interception is beyond the scope of this Note.

"connected vehicles," meaning that they wirelessly and continuously exchange data with external systems.[4] Each vehicle includes not only hundreds of sensors but also over a hundred computers to process and package the data that they collect.[5] The car then ships that data to the manufacturer, along with any raw data the vehicle cannot process onboard.[6] The output is twenty-five gigabytes of data per vehicle per hour.[7] This includes not only relatively trivial (but still valuable) information like maintenance status but also information like vehicle location, speed, heading, braking instances, and road conditions.[8] It also includes "infotainment" information—what you are listening to, what websites you access, your phone contacts, and your personal messages.[9]

---

4. OTONOMO, INVESTOR PRESENTATION 8 (2021), https://info.otonomo.io/hubfs/PDF/OOOO-PIPE-Investor-Presentation.pdf [https://perma.cc/G9TF-2K9C]; *see also* EDWARD J. MARKEY, TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 1 (2015), https://www.markey.senate.gov//imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [https://perma.cc/96E9-Z7H5] ("Nearly 100% of cars on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions.").

5. POLICE EXEC. RSCH. F., UTILIZING VEHICLE DATA IN LAW ENFORCEMENT INVESTIGATIONS 1 (2020), https://www.iacpcybercenter.org/wp-content/uploads/2020/09/Vehicle-Data_LECC-Article.pdf [https://perma.cc/ZM7F-6JR7]; *see also* FUTURE OF PRIV. F., DATA AND THE CONNECTED CAR (2017), https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf [https://perma.cc/N9KW-VCPY] (depicting the sensors and computers found on modern vehicles).

6. *Cf.* Letter from Ron Wyden, Sen., & Edward J. Markey, Sen., to Lina S. Khan, Chair, Fed. Trade Comm'n (July 26, 2024), https://www.wyden.senate.gov/imo/media/doc/wyden-markey_auto_privacy_letter_to_ftc.pdf [https://perma.cc/9SZM-PTEE] (requesting that the Federal Trade Commission investigate General Motors and other automakers for collecting and selling connected-vehicle data absent drivers' permission).

7. *E.g.*, POLICE EXEC. RSCH. F., *supra* note 5, at 1; *see also* Patrick Howell O'Neill, *Meet Berla, the Little-Known Company That Can Pull Smartphone Data from Your Car*, CYBERSCOOP (Sept. 11, 2017), https://cyberscoop.com/berla-car-hacking-dhs/ [https://perma.cc/J2RR-NVYX] (calculating that a connected vehicle creates 20 terabytes of data per person per year).

8. Daniel A. Crane, Kyle D. Logue & Bryce C. Pilz, *A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles*, 23 MICH. TELECOMM. & TECH. L. REV. 191, 207 (2017); *see also What Is Telematics?*, VERIZON CONNECT (June 26, 2023), https://www.verizonconnect.com/resources/article/what-is-telematics/ [https://perma.cc/8S4N-U4DN] ("Many modern commercial vehicle manufacturers install embedded GPS tracking and telematics technologies directly in their fleet vehicles").

9. *See* POLICE EXEC. RSCH. F., *supra* note 5, at 2 (explaining that a vehicle's infotainment and telematic systems can send, receive, and store data from text messages). Infotainment data tends to be particularly sensitive—the fine print entitles manufacturers to collect "biological characteristics," "genetic information," and "sexual activity." *See, e.g.*, GEN. MOTORS, GENERAL MOTORS U.S. CONSUMER PRIVACY STATEMENT 3 (2023), https://www.gm.com/content/dam/company/docs/us/en/gmcom/US_Consumer_Privacy_Statement_July_2023.pdf [https://perma.cc/6564-5XN9] (noting that GM vehicles collect "biological characteristics" of occupants); *Privacy Notice*, NISSAN (Jan. 1, 2023), https://www.nissanusa.com/privacy.html [https://perma.cc/9WDA-4ZB9] ("genetic information" and "sexual activity"); *Kia Connect Privacy Policy*, KIA (Aug. 27, 2024), https://owners.kia.com/us/en/privacy-policy.html#two [https://perma.cc/V7ED-TXC7] ("sex and gender information").

Smart infrastructure involves directing a sliver of connected-vehicle data to government-owned infrastructure, in real time, to promote traffic safety. This type of data is limited to location information and basic "telematic" data like speed, heading, and brake and transmission status.[10] The car uses short-range radio communications to send that data to a piece of infrastructure, such as a traffic light, bridge, overpass, highway exit, or crosswalk.[11] Once the infrastructure receives that data, it can determine if there are any hazards to that vehicle. If so, the infrastructure "talks back" to the vehicle to relay important safety information.[12] This wireless exchange of information between vehicle and infrastructures is known as vehicle-to-infrastructure, or V2I, communications.[13]

It is necessary to distinguish at the outset between the V2I communications of smart infrastructure and a closely related connected-vehicle technology: vehicle-to-vehicle communications. As the names suggest, the distinction lies in the parties involved. Vehicle-to-infrastructure technologies communicate between a vehicle and government-owned infrastructure.[14] But with vehicle-to-vehicle communications, the middleman is eliminated—two cars communicate directly.[15]

Both concepts fall under the umbrella of "connected-vehicle communications": the wireless exchange of data between a vehicle and a system external to it.[16] This technology has been the goal of transportation engineers since at least 1999, when the U.S. Department of Transportation convinced the Federal Communications Commission to reserve certain radio frequencies for connected-vehicle communications.[17] Transportation planners likely recognized the potential for these communications to push

10. Crane et al., *supra* note 8, at 200.

11. U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-775, INTELLIGENT TRANSPORTATION SYSTEMS: VEHICLE-TO-INFRASTRUCTURE TECHNOLOGIES EXPECTED TO OFFER BENEFITS, BUT DEPLOYMENT CHALLENGES EXIST 7 (2015), https://www.gao.gov/assets/680/672932.pdf [https://perma.cc/L55R-TMHL]. Engineers prefer radio- to internet-based communications due to the reliability and low latency of radio communications. *Id.*

12. *See* Crane et al., *supra* note 8, at 200 ("These roadside devices would transmit information to vehicles, enabling applications such as red light violation warnings, curve speed warnings, and weather information warnings . . . .").

13. Muhammad Naeem Tahir, Pekka Leviäkangas & Marcos Katz, *Connected Vehicles: V2V and V2I Road Weather and Traffic Communication Using Cellular Technologies*, 22 SEASONS 1142, 1142 (2022).

14. *Id.*

15. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 11, at 4–5.

16. *See How Connected Vehicles Work*, U.S. DEP'T OF TRANSP. (Feb. 27, 2020), https://www.transportation.gov/research-and-technology/how-connected-vehicles-work [https://perma.cc/EJ8K-67TM] (describing several connected-vehicle technologies and their potential to improve traffic safety).

17. *See* 64 Fed. Reg. 66405 (Nov. 26, 1999) (codified thereafter at 47 C.F.R. pts. 2, 90) (allocating "75 megahertz of spectrum at 5.850–5.925 GHz" for use by Intelligent Transportation Systems).

critical safety messages to drivers in real-time. Consider three safety applications of the technology:

- **Intersection Movement Assist.** A stop light or sign assesses a driver's speed and heading, compares it with data from nearby vehicles, and "warns the driver . . . when it is not safe to enter an intersection due to a high probability of colliding with one or more vehicles."[18] A related application is "left turn assist," which warns a driver if they are making a dangerous unprotected left turn.[19]
- **Forward Collision Warnings.** A stoplight, sign, or freestanding roadside unit compares drivers' speed and heading. The infrastructure warns drivers if it believes a collision is imminent.[20] A related application is "emergency electronic brake light warnings," which "[a]lerts the driver that a vehicle ahead is hard braking."[21]
- **Speed Violation Warnings.** Some V2I deployments, such as the Department of Transportation's pilot program in New York City, push warnings to drivers who are exceeding speed limits.[22] Other existing applications include "curve speed warnings," "reduced speed zone warnings," and "spot weather information warnings."[23]

Aspirations for the safety impacts have been high. The Department of Transportation stated that it expects connected-vehicle technologies "to reduce unimpaired vehicle crashes by as much as 80 percent."[24] It estimated that two safety applications, "intersection movement assist" and "left turn assist," could alone "prevent up to 592,000 crashes and save 1,083 lives saved per year."[25]

---

18. JOHN HARDING, GREGORY POWELL, REBECCA YOON, JOSHUA FIKENTSCHER, CHARLENE DOYLE, DANA SADE, MIKE LUKUC, JIM SIMONS & JING WANG, U.S. DEP'T OF TRANSP., DOT HS 812 014, VEHICLE-TO-VEHICLE COMMUNICATIONS: READINESS OF V2V TECHNOLOGY FOR APPLICATION 27 (2014), https://rosap.ntl.bts.gov/view/dot/27999 [https://perma.cc/YE3S-BH3L].

19. Press Release, U.S. Dep't of Transp., U.S. Department of Transportation Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communications Technology (Aug. 18, 2014), https://www.transportation.gov/briefing-room/us-department-transportation-issues-advance-notice-proposed-rulemaking-begin [https://perma.cc/R9FE-89JT].

20. HARDING ET AL., *supra* note 18, at 28.

21. INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFF., U.S. DEP'T OF TRANSP., TAMPA, FLORIDA: CONNECTED VEHICLE PILOT DEPLOYMENT PROGRAM (2019), https://www.its.dot.gov/factsheets/pdf/TampaCVPIlot_Factsheet.pdf [https://perma.cc/5NLA-KRV9].

22. *See Project Status*, N.Y.C. DEP'T OF TRANSP.: NYC CONNECTED VEHICLE PROJECT, https://cvp.nyc/project-status [https://perma.cc/6XJJ-VG3K] (noting over 7,600 "event files" uploaded to vehicles for "speed compliance").

23. HARDING ET AL., *supra* note 18, at 12.

24. INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFF., U.S. DEP'T OF TRANSP., CONNECTED VEHICLES AND YOUR PRIVACY, https://www.its.dot.gov/factsheets/pdf/Privacy_factsheet.pdf [https://perma.cc/S9UD-HKQH].

25. U.S. Dep't of Transp., *supra* note 19.

Beyond safety, advocates of connected-vehicle communications also tout the benefits of these communications to increase mobility and decrease congestion:

> V2I mobility applications could capture data from vehicles and infrastructure (for example, data on current traffic volumes and speed) and relay real-time traffic data to transportation system managers and drivers. For example, after receiving data indicating vehicles on a particular roadway were not moving, transportation system managers could adjust traffic signals in response to the conditions, or alert drivers of alternative routes via dynamic message signs located along the roadway.[26]

The ability to adjust traffic conditions would help traffic managers "[reduce] the 6.9 billion hours Americans spend in traffic annually,"[27] an effect linked to environmental considerations.[28] It would also benefit emergency services. Consider an ambulance seeking to travel down a busy street during rush hour. As a result of this technology, that vehicle would no longer have to push through bumper-to-bumper traffic. Rather, traffic system managers could clear a corridor for the ambulance by changing the signals on the stoplights between the ambulance and the hospital.[29]

Perhaps most importantly, connected-vehicle communications would assist with infrastructure and traffic planning.[30] This application involves capturing trip data with infrastructure, storing it, aggregating it, analyzing it, and deducing traffic patterns. This would help traffic managers assess

---

26. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 11, at 6.

27. INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFF., *supra* note 24.

28. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 11, at 5 (noting that V2I communications are designed to provide environmental benefits).

29. *Incorporating Connected and Autonomous Vehicles Into the Integrated Corridor Management Approach*, FED. HIGHWAY ADMIN., U.S. DEP'T OF TRANSP., https://ops.fhwa.dot.gov/publications/fhwahop17001/ch2.htm [https://perma.cc/SF85-WWCQ] (Apr. 21, 2020). Ambulances have long been outfitted with short-range radio transmitters that allow the vehicle to switch a traffic light from red to green. *See* INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFF., DEP'T OF TRANSP., TRAFFIC SIGNAL PREEMPTION FOR EMERGENCY VEHICLES: A CROSS-CUTTING STUDY, at 3-1 (2006) ("These benefits have been realized since the early deployments of [emergency vehicle preemption] and have been documented since the 1970s"). However, these are of little use if traffic is at a standstill. Once the ambulance is within range to change the signal, it must also wait for the vehicles in front of it to begin moving through the intersection. "Integrated corridor management," on the other hand, allows traffic managers to change the signals far ahead of the ambulance, ensuring that traffic is moving by the time the ambulance reaches the intersection. *Incorporating Connected and Autonomous Vehicles*, *supra*.

30. *See* BUREAU OF CONSUMER PROT., FED. TRADE COMM'N, CONNECTED CARS WORKSHOP: STAFF PERSPECTIVE 2 (2018), https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf [https://perma.cc/L2NE-Q9U9] (noting that transportation authorities will collect and analyze connected-vehicle "aggregate information [that] can be used for traffic management to reduce congestion").

friction and danger points in the traffic network.[31] For example, an analysis of traffic patterns and collisions along a residential street might convince a planning authority to install additional traffic-calming infrastructure such as speed bumps or stop signs.

This application requires storing connected-vehicle data in government-owned databases. Transportation agencies "consider themselves to be the owners of the data collected by their [V2I] sensors."[32] Once collected, V2I data becomes government records that transportation agencies use freely—either analyzing it for traffic trends in-house or sending it to "third-party data aggregators to . . . transform the data into useful information."[33] Those agencies also share it freely with other organizations.[34]

Lastly, V2I communications are critical to the development of autonomous vehicles.[35] These "self-driving" cars rely on, and come installed with, a bevy of on-board sensors.[36] However, "many vehicle automation and vehicle autonomy technologies are not feasible without electronic communications between vehicles or between vehicles and infrastructure."[37] The idea is partly that the communications provide redundancy to the on-

31. A private industry has already formed around collecting, selling, and analyzing connected-vehicle data. Manufacturers collect through onboard sensors and either analyze data in-house or "anonymize" it before selling it to a third-party. *See, e.g.*, OTONOMO, *supra* note 4, at 7, 10 (describing how Otonomo, an Israeli data broker with seventy employees, is "uniquely positioned at the heart of the automotive data ecosystem," collecting 4.3 billion data points per day).

32. JOHANNA ZMUD, MELISSA TOOLEY & MATTHEW MILLER, TEX. A&M TRANSP. INST., DATA OWNERSHIP ISSUES IN A CONNECTED CAR ENVIRONMENT: IMPLICATIONS FOR STATE AND LOCAL AGENCIES 37 (2016), https://static.tti.tamu.edu/tti.tamu.edu/documents/165604-1.pdf [https://perma.cc/YN37-7F7P].

33. *Id.* at 29. The exchange of V2I data between transportation agencies and private data aggregators is often free: The latter does not pay for the data and can use the data as desired "in exchange for useful information." *Id.*

34. *See id.* at 31 ("All of the state DOTs interviewed for this study stated that data will be shared upon request, although the conditions and mechanisms for doing so vary."); *see also id.* (noting that, at the time of the study, at least one state would share information unless police were already using it in an active investigation).

35. *See* Korok Ray & Brent Skorup, *Smart Cities, Dumb Infrastructure: Policy-Induced Competition in Vehicle-to-Infrastructure Systems*, 25 TEX. REV. L. & POL. 61, 63 (2020) ("[T]he introduction of automated vehicles onto public roads has boosted demand for high-bandwidth and supplemental wireless services, such as [connected-vehicle technologies].").

36. *See* Adam M. Gershowitz, *The Tesla Meets the Fourth Amendment*, 48 BYU L. REV. 1135, 1138 (2023) (describing the on-board capabilities of the Tesla).

37. William J. Kohler & Alex Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous, and Connected Vehicles*, 31 SANTA CLARA HIGH TECH. L.J. 99, 101 (2015). Whether this early prediction has become true is debatable. Consider that autonomous freight company, Kodiak, plans to be "driver-out" on Texas highways in the next 18 months. Interview with Dr. Anna R.W. McAuley, Senior Researcher, Ctr. for Transp. Rsch., in Austin, Tex. (Nov. 5, 2023). While Kodiak does participate in an ongoing V2I pilot, those communications are not critical to its truck's autonomous functionality. *Id.*

board sensors.[38] But the connected-vehicle communications also offer capabilities that autonomous vehicles lack. Those vehicles rely on optical sensors such as cameras and lidar.[39] By contrast, connected vehicles "talk" rather than "see." As researchers have noted, the "longer detection distance and ability to 'see' around corners or 'through' other vehicles helps [connected vehicles] perceive some threats sooner than sensors, cameras, or radar can, and warn their drivers accordingly."[40]

In summary, smart infrastructure promises to improve safety, decrease congestion, assist management and planning, and facilitate autonomous vehicle development. Each potential benefit justifies the government's strong interest in V2I adoption.

B. The V2I Data Exchange

An analysis of smart infrastructure's privacy concerns is impoverished without a thorough understanding of its underlying technology. The privacy impacts of V2I communications have been widely understated.[41] This may be because those tasked with addressing it have failed to understand precisely what is communicated and how it is valuable.

Most V2I communications use the same technology. On the vehicle, a set of computers collects data from vehicle sensors and, if needed, a supplementary GPS unit.[42] Those computers broadcast the data using an onboard radio unit over a frequency dedicated for connected-vehicle communications.[43] The broadcast typically reaches 300 meters but can go as far as one kilometer.[44] The broadcast is received by a roadside unit, which has its own radio transceiver, computer, and either fiber optic or 5G internet connectivity.[45] The roadside unit sends messages back to the vehicle in the

38. *See* HARDING ET AL., *supra* note 18, at 26 (noting that connected vehicles are "not subject to the same weather, light, or cleanliness constraints associated with vehicle-resident sensors" and thus can continue operating when those sensors are degraded due to environmental conditions).

39. *Id.*

40. *Id.* at xiv.

41. *See infra* subpart II(B). At the same time, a minority of commentators have come to the opposite conclusion; that is, connected-vehicle communications represent an enormous privacy threat. *See, e.g.*, Emilio Longoria, *Invisible, but Not Transparent: An Analysis of the Data Privacy Issues That Could Be Implicated by the Widespread Use of Connected Vehicles*, 28 ALB. L.J. SCI. & TECH., no. 1, 2017, at 1, 14 (arguing that there are "several data privacy concerns that may be implicated by widespread [connected vehicle] use"). This conclusion relies on a similar misunderstanding of the technology.

42. Crane et al., *supra* note 8, at 199–200; FUTURE OF PRIV. F., *supra* note 5.

43. Crane et al., *supra* note 8, at 199–200.

44. HARDING ET AL., *supra* note 18, at 26.

45. *See* Dorothy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J. 1617, 1633 (2014) (discussing the functional processes of V2I and V2V systems); *see also* HARDING ET AL., *supra* note 18, at 32–33 (discussing the capabilities of roadside communications systems); ITS AM., ITS AMERICA NATIONAL V2X DEPLOYMENT PLAN: AN

same manner. The vehicle communicates the message to the driver using an onboard display.[46]

The data broadcast between the vehicle and the infrastructure is not encrypted.[47] Encryption is the process of algorithmically transforming information to render it unreadable to unauthorized parties.[48] Because V2I data broadcasts are unencrypted, any radio transceiver on the correct frequency can read V2I communications data that the infrastructure receives from the vehicle.[49] This is not to say that there is no encryption involved: The data exchange between the vehicle and the infrastructure is always preceded by cryptographic authentication.[50] So, encryption ensures entity authentication but not communication confidentiality.

Put simply, a sender and receiver know that they are talking to each other, but anyone can hear their conversation. For example, Harrison's Ford and the stoplight know that they are communicating with each other, but Chase's Chevy can read their communications. The lack of confidentiality prompts the question: What is being communicated? That is, what exactly is Harrison's Ford saying that Chase's Chevy can hear?

The standard message is the Basic Safety Message (the basic message). Connected vehicles broadcast the basic message ten times per second[51] according to a pre-set format.[52] The data it sends can be conceptually divided

---

INFRASTRUCTURE & AUTOMAKER COLLABORATION 2 (2023) (describing the communication features of roadside units).

46. INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFF., *supra* note 21, at 1 (noting that vehicles are either deployed with a "dedicated display" or one integrated into the rearview mirror).

47. *See* Glancy, *supra* note 45, at 1634 ("Both parts of the Basic Safety Message are transmitted in the clear—i.e., the message is not encrypted. . . . The Basic Safety Message, containing detailed real-time vehicle location and operation information, is not itself encrypted."); *see also* EDWARD FOK, OFF. OF ASSISTANT SEC'Y FOR RSCH. & TECH, U.S. DEP'T OF TRANSP., FUNDAMENTAL PRIVACY CONCEPTS FOR THE CONNECTED VEHICLE DEPLOYMENTS 15–16 (2015), https://www.its.dot.gov/pilots/pdf/CVP_TechAssistWebinar_Privacy_v4.pdf [https://perma.cc/U763-RVWT] (noting that secured credentials are used for authentication, not message content).

48. *See* KEITH STOUFFER, MICHAEL PEASE, CHEEYEE TANG, TIMOTHY ZIMMERMAN, VICTORIA PILLITTERI, SUZANNE LIGHTMAN, ADAM HAHN, STEPHANIE SARAVIA, ASLAM SHERULE & MICHAEL THOMPSON, U.S. DEP'T OF COM., NIST SP 800-82r3, GUIDE TO OPERATIONAL TECHNOLOGY (OT) SECURITY 162 (2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf [https://perma.cc/9FU4-WPSS] (providing a technical definition of "encryption").

49. *See* Glancy, *supra* note 45, at 1635 (describing some of the security risks involved with unencrypted connected-vehicle communications).

50. HARDING ET AL., *supra* note 18, at 158, 160 n.226. This procedure uses public-key encryption. *Id.* at xviii; NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., FMVSS NO. 150, VEHICLE-TO-VEHICLE COMMUNICATION TECHNOLOGY FOR LIGHT VEHICLES, at III-5 (2016), https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/v2v_pria_12-12-16_clean.pdf [https://perma.cc/92FT-T9PT].

51. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 11, at 5.

52. *See* FOK, *supra* note 47, at 8 (listing broadcast format for radio, authentication, and data vocabulary); *see also* SAE INT'L, SURFACE VEHICLE STANDARD: V2X COMMUNICATIONS

into telematic and location information. At a minimum,[53] the telematic information includes vehicle speed, heading, steering wheel angle, brake status, transmission status (whether the vehicle is in drive, park, or reverse), and acceleration.[54] The location information in the basic message includes the vehicle's longitude, latitude, and elevation.[55] Location is extremely accurate—latitude and longitude are specified to the tenth of a microdegree.[56]

Aside from telematic and location data, each basic message includes two other notable pieces of information. First, each message sends with a number that identifies the vehicle transmitting it.[57] This identification number is temporary and one of over four billion possible values.[58] According to the connected-vehicle standard, "[t]he circumstances and times at which [vehicles] create and change their current temporary [identification number] is a complex application level topic."[59] In other words, how long vehicles retain their temporary identification number depends on how they are configured. But the intent is that the temporary identification number "will periodically change to a new random value to ensure the overall anonymity of the vehicle."[60] While the standard is ambiguous, vehicles in current V2I deployments retain the same temporary identification number for at least thirty minutes.[61]

MESSAGE SET DICTIONARY 12 (2023), https://www.sae.org/standards/content/j2735_202309/ [https://perma.cc/EAN9-BL6L] ("This SAE Standard specifies a message set, and its data frames and data elements, for use by application that use vehicle-to-everything (V2X) communications systems.").

53. There are some fields that are considered supplemental, meaning that the on-board units will transmit that data if the user or manufacturer configures it to do so. SAE INT'L, *supra* note 52, at 33. One supplemental of a data field is for "path history." *Id.* at 86. This data is very short-term and cannot be effectively used to recreate a vehicle's trip. *See id.* (noting that the path history data frame holds a maximum of 23 points). For example, a vehicle may transmit path history over the course of a turn. This allows a piece of infrastructure to better predict vehicle path than it would with the heading and steering angle alone.

54. SAE INT'L, *supra* note 52, at 49, 214, 260.

55. *Id.* at 259.

56. *Id.* at 163–64.

57. *See id*. at 208 (describing the use of a "TemporaryID" that is used to identify local vehicles).

58. The temporary identification number is 4 bytes, *id.*, meaning it is one of 4,294,967,296 possible values. Paul Murrell, *Computer Memory*, STAT MATH § 7.4, https://statmath.wu.ac.at /courses/data-analysis/itdtHTML/node55.html [https://perma.cc/RM4B-VEZ3]. That suggests that the number a vehicle uses is almost guaranteed to be unique.

59. SAE INT'L, *supra* note 52, at 208.

60. *Id.*; *see also* FOK, *supra* note 47, at 20 (claiming that the time-based expiration of the credentials prevents a data analyst from tracking a single vehicle); DREW VAN DUREN, SCOTT CADZOW, JONATHAN PETIT, WILLIAM WHYTE & ROBERT RAUSCH, U.S. DEP'T OF TRANSP., FHWA-JPO-17-453, CONNECTED VEHICLE PILOT DEPLOYMENT PROGRAM PHASE 2: DATA PRIVACY PLAN—NEW YORK CITY 14, 34 (2016), https://rosap.ntl.bts.gov/view/dot/32311 [https://perma.cc/GTS6-NG5L] (stating that the temporary identification number will change "from time to time" to "prohibit tracking a single vehicle").

61. *See infra* subpart II(B).

Second, the basic message sends the size of the vehicle.[62] This includes both the length and width of the vehicle, measured in centimeters.[63]

The total package of a V2I basic message is thirty-eight bytes.[64] This is a very compact data package—smaller than the preceding sentence.[65] Its size is one of the reasons that a connected vehicle can easily broadcast it ten times per second.[66] That innovation, along with low hardware demands, is one of the reasons why transportation engineers increasingly deploy V2I.[67]

C. Current V2I Deployments

Ongoing connected-vehicle pilot programs demonstrate the potential for V2I technology to improve traffic safety and congestion. Implementation of V2I communications on public roadways began in earnest with three U.S. Department of Transportation pilot deployments in 2015.[68] The first was a partnership with New York City, which saw the city install 470 receivers on infrastructure across Manhattan and Brooklyn.[69] The city also outfitted 3,000 of its vehicles (buses, trucks, and passenger vehicles) with connected-vehicle technology.[70] The second pilot was in Tampa Bay, Florida, where the transit authority similarly outfitted 1,035 vehicles and forty-seven intersections.[71] Unlike the New York deployment, Tampa's mostly consisted of private passenger vehicles[72] with alert displays integrated into their rearview mirrors.[73] The final partner for this federal deployment, the State of Wyoming, focused its efforts on freight.[74] Wyoming installed 327 units in commercial trucks and government-owned snowplows, as well as seventy-

62. SAE INT'L, *supra* note 52, at 50.

63. *Id.* at 218, 221. The specificity of this measurement assists in inferring not only the type of vehicle sending the message but also the exact make and model.

64. FOK, *supra* note 47, at 15.

65. One character is one byte in the standard ACII encoding. BHARAT KINARIWALA & TEP DOBRY, PROGRAMMING IN C[1] 140 (1993). The preceding sentence is sixty-three characters, so the sentence is sixty-three bytes of information.

66. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 11, at 5 (noting that the basic message transmits ten times per second under typical conditions).

67. *See, e.g.*, KATE HARTMAN, KARL WUNDERLICH, MEENAKSHY VASUDEVAN, KATHY THOMPSON, BARBARA STAPLES, SAMPSON ASARE, JAMES CHANG, JUSTIN ANDERSON & ATIZAZ ALI, U.S. DEP'T OF TRANSP., FHWA-JPO-23-990, ADVANCING INTEROPERABLE CONNECTIVITY DEPLOYMENT: CONNECTED VEHICLE PILOT DEPLOYMENT RESULTS AND FINDINGS 1 (2023), https://rosap.ntl.bts.gov/view/dot/68128 [https://perma.cc/78N3-XS9C] (describing a recent deployment of V2I communications in New York City, New York; Tampa, Florida; and Wyoming).

68. *See id*. (describing current V2I technology deployments).

69. *Id.* at 8.

70. *Id.*

71. *Id.* at 9–10.

72. *Id.*

73. INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFF., *supra* note 21, at 1.

74. HARTMAN ET AL., *supra* note 67, at 7.

six roadside units along a 402-mile corridor of highway running through the state.[75]

These deployments demonstrated the potential of connected-vehicle communications. Wyoming saw outfitted vehicles reduce their speeds by 50%.[76] Those vehicles also "talked back" to the infrastructure by notifying it when road conditions were poor; the state's road condition reports increased by 400%.[77] Drivers in the Tampa pilot saw their travel times decrease by 30%.[78] New York reported a significant reduction in vehicle emissions.[79]

Partly due to the perceived success of this deployment, as well as more federal dollars for V2I,[80] other pilot programs have followed suit. The Department of Transportation began another V2I pilot program focused on smart signals, with 2,000 signals installed across twenty-six states.[81] In Texas, a state-run connected-vehicle pilot focusing on commercial freight works with autonomous trucking companies to communicate between 1,000 trucks and central Texas highways.[82] The City of Austin is experimenting with V2I crosswalks.[83] The University of Michigan recently announced that

75. *Id.*

76. *Id.* at 14 fig.13.

77. *Id.* at 14 fig.13, 30.

78. *Id.* at 14 fig.13.

79. *Id.* New York published its event data for its pilot. *See Project Status*, *supra* note 22 (showing alert statistics transmitted in December 2021). Interestingly, almost half of the nearly 16,000 warnings pushed to drivers were for speeding. *Id*.

80. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 11, at 14 (reporting that the Department of Transportation planned to allocate $100 million toward developing connected-vehicle technologies from 2015–2020).

81. INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFF., U.S. DEP'T OF TRANSP., ITS DEPLOYMENT EVALUATION: SIGNAL PHASE AND TIMING (SPaT) 2 (2020), https://www.itskrs.its.dot.gov/sites/default/files/2021-09/executive-briefing/07_SPaT%20Challenge_FINAL%20508%20VERSION_06_23_21.pdf [https://perma.cc/Z43D-HUUZ].

82. *See* TEX. DEP'T OF TRANSP., TEXAS CONNECTED FREIGHT CORRIDORS: A SUSTAINABLE CONNECTED VEHICLE DEPLOYMENT 1–2 (2017), https://ftp.dot.state.tx.us/pub/txdot-info/trf/freight-corridors/proposal.pdf [https://perma.cc/MC6L-J434] (describing the currently ongoing V2I pilot in an application for almost $8 million of federal funding). This program has been particularly successful. The program managers seek to expand it to the U.S.–Mexico border, where they hope to use connected-vehicle data exchanges to "create a virtual or physical traffic operations center . . . to share real-time information between Mexican" and American authorities. NICK WOOD, PAUL ANDERSON, MINH LE, DAN MIDDLETON, ROBERT SAYLOR & JEFFREY WARNER, TEX. A&M TRANSP. INST., POTENTIAL APPLICATIONS TO EXPAND THE TEXAS CONNECTED FREIGHT CORRIDORS SYSTEM 4 (2022), https://static.tti.tamu.edu/tti.tamu.edu/documents/0-7125-R1.pdf [https://perma.cc/YPY8-WN5J].

83. Jason JonMichael, *Pilot Programs in Austin, Texas Leveraging Technology to Meet Vision Zero Goals*, ROADS & BRIDGES (Oct. 18, 2021), https://www.roadsbridges.com/road-traffic-safety/article/10654364/pilot-programs-in-austin-texas-leveraging-technology-to-meet-vision-zero-goals [https://perma.cc/886X-R9JC]; *see also Emerging Mobility Technology*, CITY OF AUSTIN, https://www.austintexas.gov/department/smart-mobility#:~:text=,Austin%20Mobility%20News%3A%20Austin%27s [https://perma.cc/532A-NGKR] (discussing the implementation of the TAPCO pedestrian crosswalk warning system).

it would expand a long-running vehicle-to-vehicle communications pilot in the City of Ann Arbor.[84] And America is not the only testbed for connected vehicles—Japan has long been a pioneer of the technology.[85]

The future is bright for V2I technologies, and momentum is in favor of widespread adoption. Indeed, the network effects of adoption are a primary reason that proponents are so optimistic. The greater number of vehicles communicating in a V2I system, the more information exchanged, and the more informed infrastructure will be. With a broader base of information coming from more vehicles, infrastructure can issue more (and more precise) warnings. This will enable safety benefits to far exceed those demonstrated by the existing pilots.[86]

Recognizing the potential for network effects to supercharge connected-vehicle benefits, the National Highway Traffic Safety Administration (NHTSA), a component of the Department of Transportation, has sought to use its regulatory muscle to encourage adoption. Specifically, the NHTSA proposed a federal rule in 2017.[87] That rule would require that all passenger vehicles are sold with the onboard technology necessary for connected-vehicle communications.[88] The consensus view is that this rule would be firmly within the NHTSA's authority to regulate vehicle safety equipment.[89]

These deployments underscore that transportation authorities recognize the potential for V2I communications to improve traffic safety and

84. Jim Lynch, *$9.8M to Boost Connected Vehicle Research and Expand Ann Arbor Deployment*, MICH. ENG'G NEWS (May 25, 2023), https://news.engin.umich.edu/2023/05/9-8m-to-boost-connected-vehicle-research-expand-ann-arbor-deployment/ [https://perma.cc/TF67-MLA6].

85. *See* HARDING ET AL., *supra* note 18, at 118 (discussing the connected-vehicle technological advances Japan was making in 2014).

86. *See* Crane et al., *supra* note 8, at 238 ("[I]n order to provide significant crash avoidance benefits, a connected-vehicle system requires a critical mass of connected vehicles on the road.").

87. Federal Motor Vehicle Safety Standards: V2V Communications, 82 Fed. Reg. 3854 (Jan. 12, 2017) (to be codified at 49 C.F.R. pt. 571). This rule remains pending, and its future is uncertain. *See infra* subpart III(B) and accompanying text.

88. Crane et al., *supra* note 8, at 303 ("NHTSA's [proposal] would require vehicle-based hardware such as DSRC radios, a GPS receiver with a process, an inertial measurement unit, and a driver-vehicle interface.").

89. *See, e.g.*, *id.* at 303–04 (explaining that it is "relatively clear" that NHTSA has statutory authority to regulate onboard connected-vehicle hardware, given "that such infrastructure is likely a device 'manufactured . . . with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death' and therefore motor vehicle equipment under § 30102(a)(7)(C) of the Safety Act" (alteration in original) (quoting 49 U.S.C. § 30102(a)(8)(C)(ii))). Notably, federal authority may end with requiring installation of onboard connected-vehicle equipment. The Department of Transportation may not have the authority to directly install, or compel states and municipalities to install, V2I equipment on infrastructure. Perhaps recognizing this, the Department has only stated that municipalities are "strongly encouraged" to install V2I equipment. *Id.* at 305; *see also* FED. HIGHWAY ADMIN., 2015 FHWA VEHICLE TO INFRASTRUCTURE DEPLOYMENT GUIDANCE AND PRODUCTS: V21 GUIDANCE DRAFT V9A, at 3 (2014) ("Deployment of [V2I] services will be strongly encouraged by the [Federal Highway Administration], but will be voluntary.").

congestion. But they are not the only government agencies eyeing this capability.

II. Even If You Build It "Anonymous," They Will Still Come

A common concept in privacy is "if you build it, they will come."[90] The idea is that whenever an organization collects sensitive personal information, law enforcement will eventually seek to access that information to investigate crime.[91] Despite claims that the data that the V2I communications exchange is not sensitive, law enforcement can and will seek to use it for criminal investigation.[92]

A. V2I Proponents Claim that the Communications Preserve Anonymity

Proponents of V2I communications repeatedly emphasize that those communications are anonymous. They recognize that "communicating location and other data back and forth over a wireless network could be very useful tools for invisible targeted surveillance."[93] As a result, connected-vehicle technologies have been "painstakingly designed to maximize anonymity and neither to create nor to collect personal information."[94] As stated by the NHTSA: "There is no data in the safety messages exchanged by vehicles or collected by [connected-vehicle systems] that could . . . personally identify a . . . driver."[95] This is due to the format of the data exchange.[96] According to the NHTSA, that format ensures that "tracking a specific car or driver based on [basic messages] would be both difficult and

90. *See* Jennifer Valentino DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/2CNT-BBYA] (noting "a phenomenon privacy advocates have long referred to as the 'if you build it, they will come' principle—anytime a technology company creates a system that could be used in surveillance, law enforcement inevitably comes knocking").

91. *See* Julia Love, *Self-Driving Car Footage Gives Police Controversial New Tool*, BLOOMBERG L. (June 29, 2023, 9:00 AM), https://news.bloomberglaw.com/white-collar-and-criminal-law/as-googles-waymo-expands-so-does-a-police-surveillance-tool [https://perma.cc/TF7L-3SV7] ("Whenever you have a company that collects a large amount of data on individuals, the police are eventually going to come knocking on their door hoping to make that data their evidence." (quoting Matthew Guariglia, Elec. Frontier Found.)).

92. *See* Glancy, *supra* note 45, at 1649 ("Law enforcement access to connected vehicles and their data seems inevitable.").

93. Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1210 (2012); *see also* FOK, *supra* note 47, at 11 (describing vehicle data as "locational" information "that can be used to track an individual at a particular location").

94. Glancy, *supra* note 45, at 1658.

95. HARDING ET AL., *supra* note 18, at 144.

96. *See id.* at 154 (describing the difficulty of analyzing the basic messages).

costly."[97] The result is only "very limited potential risks to individual privacy."[98]

Similarly, the Department of Transportation's Intelligent Transportation Systems Office has stated that the basic message does not "contain data that is reasonably, or as a practical matter, linkable to you."[99] Further, the Office stated, "[t]hird parties attempting to use the [connected-vehicle] system to track a vehicle would find it difficult to do so, particularly in light of simpler and cheaper means available for that purpose."[100] Or as a legal commentator put it, the basic message "is not identified with regard to any particular vehicle or person, [so] the task of re-identification would be particularly difficult, time-consuming, and costly. Securing a judicial warrant to install a GPS device on a suspect's vehicle . . . would almost certainly be less expensive and less burdensome."[101]

But the idea that V2I communications "will not permit tracking through space or time of vehicles"[102] or "cannot be used to recreate accident scenes"[103] seems dubious. This is particularly true considering how much publicly available information can aid identification.

B. "Anonymous" Data Is Still Useful to Police

Criminal investigators know that that there is no such thing as truly anonymous data, so they are watching eagerly to see how V2I technologies develop. Indeed, the data transferred through V2I communications suggests that deanonymization is trivial and the privacy risks are real. The basic message that each vehicle transmits includes telemetry and location data. It pairs that information with a temporary identification number for the vehicle.[104] According to the industry standard for V2I applications, each connected vehicle broadcasts this data unencrypted every ten milliseconds.[105] In theory, this information can be tied to a specific vehicle to recreate its trip through connected infrastructure.

---

97. *Id.*

98. *Id.*

99. INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFF., *supra* note 24.

100. *Id.*

101. Glancy, *supra* note 45, at 1654.

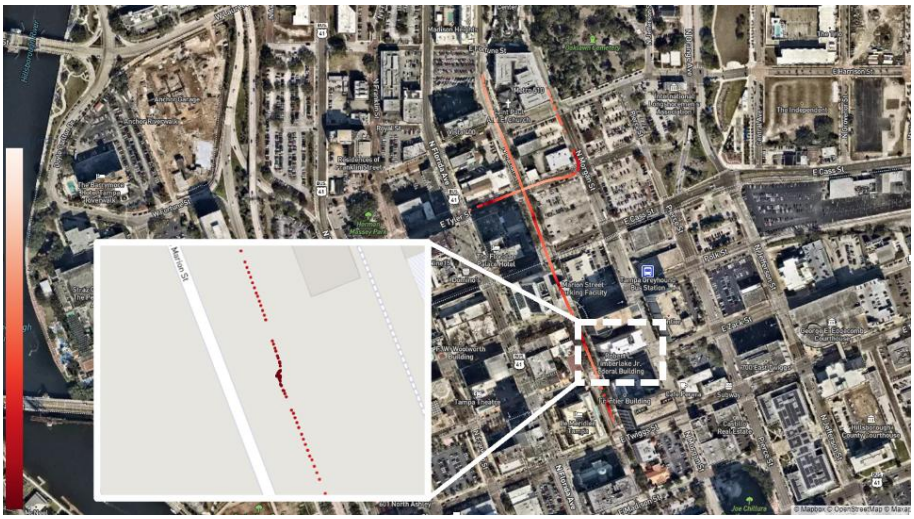
102. HARDING ET AL., *supra* note 18, at 144.

103. BOB RAUSCH, TRANSCORE, CONNECTED VEHICLE DEPLOYMENT CHALLENGES & LESSONS LEARNED IN NYC 13 (2019), https://transops.s3.amazonaws.com/uploaded_files/Deployment%20Lessons%20Learned%20NOCoE%20FINAL.pdf [https://perma.cc/C6ZX-SEL2].

104. *See supra* notes 57–61 and accompanying text.

105. SAE INT'L, *supra* note 52, at 33.

A test using V2I pilot data proves this theory. That is, it proves almost trivial to deanonymize a single vehicle using basic message data.[106] Consider a single day of basic messages that are exchanged in Tampa Bay's V2I deployment.[107] The set includes thousands of individual basic messages. Those messages can be matched up by the temporary identification number.[108] Then, considering that each basic message includes location information, each message can be plotted on a map. The map below demonstrates what this looks like.



In the plot above, all messages were captured by a single receiver on a smart traffic light. While the Department of Transportation dictates that vehicles will change their temporary identification number "from time to

106. The computer code for the demonstration that follows is available on the Author's GitHub page. *See* tmca43, *Deanonymize Tampa Bay Pilot Data*, GITHUB (Nov. 24, 2023), https://github.com/tmca43/connected-vehicle-deanonymization/blob/main/tampabay.ipynb [https://perma.cc/7APC-G7G9] (assessing claims that V2I communications preserve the anonymity of drivers). A deeper discussion of the steps involved and interactive visualizations are available on the Author's website. *Tracking Drivers with Smart Infrastructure*, TPM DATA (Jan. 28, 2024), https://www.tpmdata.com/posts/tracking-drivers-with-smart-infrastructure [https://perma.cc/Q2BT-N5XA].

107. *See Tampa CV Pilot Basic Safety Message (BSM) Sample*, U.S. DEP'T OF TRANSP. (Apr. 30, 2024), https://data.transportation.gov/Automobiles/Tampa-CV-Pilot-Basic-Safety-Message-BSM-Sample/nm7w-nvbm [https://perma.cc/ZUN3-GCAS] (analyzing a dataset from March 1, 2021); HARTMAN ET AL., *supra* note 68, at 9–10 (describing how the Tampa Bay deployment outfitted over 1,000 mostly private vehicles).

108. *See supra* notes 57–58 and accompanying text.

time,"[109] this dataset shows that the same identification number is retained for at least thirty minutes.[110]

Basic inferences from the data enable deanonymization. Each of the basic messages plotted above state that the vehicle has a width of 254 centimeters and length of 1,250 centimeters.[111] This confirms that we are dealing with the same vehicle. But those dimensions are much larger than a passenger vehicle,[112] suggesting that the vehicle is a commercial truck or bus. Additionally, as evidenced in the map above, the vehicle pulled to the right side of the road to stop at a midblock location for 50 seconds.[113] This suggests that the vehicle was a bus. The vehicle stopped at that location at 6:28 AM.[114] The departure board on Google Maps shows that bus route 9 is scheduled to pick up from that location at 6:27 AM, which matches the observed pattern.[115] We can compare those routes against the remaining locations sent by the basic messages. That reveals that this vehicle was the Hillsborough Area Region Transit number 9 bus.[116]

This level of deanonymization is far from "difficult and costly."[117] But it is nonetheless valuable for criminal investigations. Consider if police

109. VAN DUREN ET AL., *supra* note 60, at 14.

110. *Tracking Drivers with Smart Infrastructure*, *supra* note 106.

111. *See* tmca43, *supra* note 106 (displaying and isolating vehicle sizes in cells 97 and 98).

112. *Automobile Dimensions and Sizes of All Makes*, AUTOMOBILEDIMENSION.COM, https://www.automobiledimension.com/car-search-engine.php [https://perma.cc/S7DS-RNSS].

113. *See Tracking Drivers with Smart Infrastructure*, *supra* note 106 (noting in an interactive visualization that the vehicle stopped between Polk Street and E. Zack Street from 6:27:50 AM to 6:28:40 AM).

114. *Id.*

115. Bus Stop Schedule for Marion Street @ Zack Street, GOOGLE MAPS, https://www.google.com/maps [https://perma.cc/3ZH9-XJZH]. To find the 6:27 AM pick-up time, search Tampa, Florida; then search Marion St @ Zack St; then click "See departure board" under "Buses"; and then scroll until listings around 6:27 AM appear.

116. *Compare Route 9*, HILLSBOROUGH AREA REG'L TRANSIT (Aug. 9, 2024), https://www.gohart.org/Route/Route%2009%20-%20080424.pdf (showing the Route 9 schedule), *with Tracking Drivers with Smart Infrastructure*, *supra* note 106 (showing an identical route north to the Marion Transit Center).

The fact that we can reach this level of identification given 30 minutes and "anonymous" data may be unsettling given the impending implementation of V2I technology. But there is a tradeoff between privacy and functionality when structuring data exchanges. If you make the data totally resistant to deanonymization, you lose functionality. A vehicle message that only says "I am a vehicle" cannot be used to deanonymize its sender, but it is useless for improving safety. *See* Lauren Smith, Remarks at Federal Trade Commission Connected Cars Workshop: Privacy, Security Issues Related to Connected, Autonomous Vehicles (June 28, 2017), https://www.ftc.gov/media/71189 [https://perma.cc/9AE5-AAZU] ("[H]aving more data is often critical to enhancing safety . . . . [S]o how we approach some of these standard privacy principles may wind up needing to be a little bit different in the car space.").

117. The steps above took the Author (a novice programmer) half an hour. Moreover, matching basic message data to a connected vehicle is also not the only way of deanonymizing a vehicle. The basic messages are preceded by cryptographic authentication, which includes additional data that itself can aid deanonymization. *See* Lindsey Barrett, *Herbie Fully Downloaded: Data-Driven*

layered this information with additional data. Law enforcement could identify specific individuals and reconstruct their trips. Even when vehicles' temporary identification numbers change, the specificity and frequency of location data would make matching identification numbers straightforward.[118]

Moreover, the above exercise only made use of location data. But the basic messages also include telematic information.[119] Imagine the following scenario: A smart crosswalk collects information associated with a single vehicle when it approaches the crosswalk late at night. The telemetry data indicates the vehicle was swerving and speeding. Then the vehicle's brakes engaged. It came to a hard stop in the crosswalk. Its brakes remained engaged for five seconds before the transmission shifted to reverse. The vehicle moved backwards a few meters. It then drove forward, maneuvered to the left, and corrected its heading after passing the crosswalk. It sped off and turned at the next intersection.

If the police later receive a call that a person was struck by a vehicle in that crosswalk, the V2I telematic data would provide strong evidence of a hit-and-run. It may also help with the investigation: The driver turned at the next intersection, so video surveillance along that road may help identify him.

Police recognize the promise of connected-vehicle technologies for their investigative work.[120] Investigators have long relied on information collected from manufacturers about vehicle locations.[121] Those manufacturers, who track vehicle location and telematics for advertising and data brokerage, have long complied with law enforcement requests for

Vehicles and the Automobile Exception, 106 GEO. L.J. 181, 191 (2017) (noting that "pervasive tracking could still be possible by linking a vehicle's [basic messages] to identified cryptographic certificates").

118. If a vehicle with Temporary Identification Number 1 is transmitting from Point A, then 10 milliseconds later, a vehicle transmits with Temporary Identification Number 2 from Point A, the connection is simple.

119. *See supra* subpart I(B).

120. *See, e.g.*, *Traffic Safety: Automated & Connected Vehicles/V2X*, NAT'L SHERIFFS' ASSOC., https://www.sheriffs.org/trafficsafety/automated [https://perma.cc/JXG5-Y9P4] ("The emerging technology of automated and connected vehicles promises to have a positive impact on traffic safety making streets safer across the country."); POLICE EXEC. RSCH. F., *supra* note 5, at 1 ("[V]ehicle data has become an invaluable source of digital evidence and can help law enforcement investigators piece together the key 'who, what, where, and when' of their investigations.").

121. Thomas Brewster, *Cartapping: How Feds Have Spied on Connected Cars for 15 Years*, FORBES (Jan. 15, 2017, 4:30 PM), https://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/?sh=15ebdacf2ef8 [https://perma.cc/P8VQ-FTAB].

information.[122] Warrants often accompany those requests.[123] But sometimes they do not.[124]

Connected-vehicle communications would at least supplement, if not obviate, the need to work with manufacturers. Why would a detective seek a warrant for a manufacturer's data if he can get the same information by asking the city's traffic manager?

III. The Fourth Amendment and Smart Infrastructure

The Fourth Amendment to the Federal Constitution guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[125] When assessing potential violations of the Fourth Amendment, a court first must ask the "threshold question" of whether the challenged government action was a search.[126] If the conduct was a search and was not authorized by a warrant, then it is a per se Fourth Amendment violation.[127] But the government can rebut a presumed Fourth Amendment violation if the search was nonetheless reasonable.[128] As the Supreme Court has expounded, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[129]

---

122. *Id.*

123. *See, e.g.*, Order to Comply with Roving Interception of Oral Communications at 2–3, *In re* Application of the U.S., No. 2:01-cv-01495 (D. Nev. Dec 19, 2001) (compelling an early vehicle monitoring service to "monitor oral communications" inside a suspect's vehicle and convey the conversations to the FBI); Order Denying Defendant's Motion to Suppress Evidence at 6–7, United States v. Coleman, No. 2:07-cr-20357 (E.D. Mich. Feb. 20, 2008) (denying suppression motion of evidence collected from an OnStar connected-vehicle system); Motion to Suppress Illegally Obtained Evidence and Statements by Defendant 5–6, United States v. Dantzler, No. 3:10-CR-00024 (W.D. La. Mar. 31, 2010) (seeking to suppress evidence collected from vehicle monitoring system).

124. Jen Caltrider, Reem Suleiman, Misha Rykov & Zoë MacDonald, *"Is This Even Legal?" Our Top Cars-and-Privacy Question, Answered*, MOZILLA FOUND. (Feb. 29, 2024), https://foundation.mozilla.org/en/privacynotincluded/articles/is-this-even-legal-our-top-cars-and-privacy-question-answered/ [https://perma.cc/LV2D-G3M2] (studying twenty-five car manufacturers to determine that 56% share data with the government when they receive an "informal request").

125. U.S. CONST. amend. IV.

126. Carpenter v. United States, 138 S. Ct. 2206, 2215 n.2 (2018); *see also* New Jersey v. T.L.O., 469 U.S. 325, 335 (1985) (noting that the Court "has never limited the Amendment's prohibition on unreasonable searches and seizures to operations conducted by the police"). The Court's refusal to hold that the Fourth Amendment applies only against police is significant here; transportation agencies and transit authorities, not police, collect V2I communications.

127. *See* Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment . . . .").

128. *See* Carroll v. United States, 267 U.S. 132, 147 (1925) ("The Fourth Amendment does not denounce all searches or seizures, but only such as are unreasonable.").

129. Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

Given the inevitability of widespread connected-vehicle communications, a court will one day assess whether the *collection* of V2I communications is lawful under the Fourth Amendment.[130] Existing law suggests that it is. But that conclusion will not end the analysis. Police will inevitably search through these collected communications to gather evidence. Thus, a future court will also need to consider whether *police access* to collected V2I communications—such as by querying a V2I database—warrants its own Fourth Amendment protection. While courts have traditionally refused to find that querying a database is itself a Fourth Amendment search, trends in the case law suggest that they are increasingly willing to do so. How a court will decide this question in a future with ubiquitous V2I systems is unclear.

This Part will consider both of these Fourth Amendment questions. It focuses first on collection: Is collecting drivers' V2I data a search under the Fourth Amendment? Assuming that it is, this Part then asks whether that search is reasonable and thus permissible. This Part concludes by considering police access: Is the government's subsequent search through those collected communications—in the form of a database query—itself a Fourth Amendment event that must be reasonable?

A. Collecting V2I Communications Should Not Be a Fourth Amendment Search

Collecting V2I communications is not a Fourth Amendment search because it involves no trespass or violation of a reasonable expectation of privacy. Given a claimed violation of Fourth Amendment rights, a court must first assess whether the challenged conduct constituted a search.[131] Two lines of analysis support that inquiry. Under a trespass-based approach, the Court has held that a search occurs when the government "obtains information by physically intruding on a constitutionally protected area."[132] Alternatively, a search occurs when the government encroaches into an area over which a person has "exhibited an actual (subjective) expectation of privacy . . . that

130. *See* Glancy, *supra* note 45, at 1649 ("Law enforcement access to connected vehicles and their data seems inevitable.").

131. *See, e.g.*, *Katz*, 389 U.S. at 353–54 (deciding the challenged conduct was a search before assessing the "question remaining for decision [of] whether the search . . . complied with constitutional standards").

132. United States v. Jones, 565 U.S. 400, 406 n.3 (2012). These areas include "persons, houses, papers, and effects." U.S. CONST. amend. IV. A court could potentially consider sensitive personal data (a category that could itself include V2I data) to be an "effect." *See* Carpenter v. United States, 138 S. Ct. 2206, 2267–72 (2018) (Gorsuch, J., dissenting) (suggesting cellular location information is one's paper or effect under the Fourth Amendment). For discussion of potential legislative involvement, see *infra* note 261 and accompanying text. At present, the law to support this conclusion is underdeveloped. *See infra* note 261 and accompanying text.

society is prepared to recognize as 'reasonable.'"[133] This latter test has been criticized as circular and hard to apply.[134] However, as the Court has noted when assessing the Fourth Amendment lawfulness of GPS tracking through the physical installation of a device, "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."[135] So, the *Katz* framework governs whether the collection of wireless V2I communications is a search.[136]

That framework includes two components. First, the subjective: Has the person "exhibited an actual (subjective) expectation of privacy"?[137] Second, the objective: Is that expectation one "that society is prepared to recognize as 'reasonable'"?[138] Both components are relevant to the Fourth Amendment's application here and are thus addressed in turn.

1. Drivers Do Not Exhibit a Subjective Expectation of Privacy in V2I Telematic Data.—In analyzing whether a search occurred under the *Katz* framework, a court first assesses whether the party claiming a Fourth Amendment search had "an actual (subjective) expectation of privacy" over

133. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

134. Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The *Katz* test . . . has often been criticized as circular, and hence subjective and unpredictable."); *see also* Kohler & Colbert-Taylor, *supra* note 37, at 124 (noting in a pre-*Carpenter* article that "[t]he application of the reasonable expectation of privacy test has been unpredictable in the past, and it is not clear whether such a reasonable expectation of privacy will be found to exist with respect to vehicular location information" (citation omitted)).

135. United States v. Jones, 565 U.S. 400, 410–11 (2012); *see also id.* at 415 (Sotomayor, J., concurring) ("In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the . . . trespassory test may provide little guidance."); Smith v. Maryland, 442 U.S. 735, 739 (1979) ("In determining whether a particular form of government-initiated electronic surveillance is a 'search' within the meaning of the Fourth Amendment, our lodestar is *Katz v. United States*." (citation omitted)).

136. This is despite the Court's statement in *Jones* that "[i]t is beyond dispute that a vehicle is an 'effect' as that term is used in the [Fourth] Amendment." *Jones*, 565 U.S. at 404. Consider that a potential search using V2I collection relies on owner- or manufacturer-installed hardware, while police installed the hardware in *Jones*. *Id.* at 402–03. But the trespass-based approach used in *Jones* does control in a closely related vehicle-data context: vehicle "black boxes." *See, e.g.*, Mobley v. State, 834 S.E.2d 785, 793 (Ga. 2019) (holding that the physical "retrieval of data from [a car's computer] . . . without a warrant was an unreasonable search and seizure that violated the Fourth Amendment"); State v. Worsham, 227 So. 3d 602, 608 (1Fla. Dist. Ct. App. 2017) (describing black box data as "difficult to access" and finding a "reasonable expectation of privacy" in it), *cert. denied*, 138 S. Ct. 264 (2017); Gershowitz, *supra* note 36, at 1144 n.46 ("To access the [vehicle's black box], police must either rip up the carpet from inside the vehicle or insert a device into a port under the steering wheel. Either of those actions would seemingly be a trespass."); BILL CANIS & DAVID RANDALL PETERMAN, CONG. RSCH. SERV., R43651, "BLACK BOXES" IN PASSENGER VEHICLES: POLICY ISSUES 3–4 (2014) (describing the value of black-box data for law enforcement, automakers, and transportation planners).

137. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

138. *Id.*

the information that the government obtained.[139] "In determining whether a defendant held a subjective expectation of privacy, [courts] look at the defendant's efforts to conceal and keep private that which was the subject of the search."[140] A defendant may show such an effort by "[taking] normal precautions to maintain his privacy."[141] "[B]ut objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."[142]

Putting aside for the moment the location information that V2I systems transmit,[143] there are three reasons why a court should hesitate to find that connected-vehicle drivers exhibit a subjective expectation of privacy over the *telematic* data that they exchange with infrastructure.

First, connected-vehicle drivers broadcast this data repeatedly and frequently to anyone who will listen.[144] As one commentator phrased it: "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, [connected vehicles] will broadcast the information they collect like a radio—where anybody can tune in."[145] This mode of communication is analogous to posting to a public social media account or shouting on the streetcorner. As the *Katz* majority stated, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[146]

Second, this type of data is broadcast unencrypted.[147] Not only does this mean that the data is available for any third party to read, but the fact that the sender does not encrypt it suggests that they do not believe it to be private. Granted, connected-vehicle drivers do not decide whether the industry-standard message format dictates the messages are sent encrypted. But those drivers also may still know that the messages lack encryption, so their continued use of V2I communications suggests that they consent to their lack of confidentiality. In effect, a connected-vehicle driver "assume[s] the risk that the information would be divulged to police."[148]

---

139. *Id.*

140. United States v. Villegas, 495 F.3d 761, 767 (7th Cir. 2007).

141. California v. Ciraolo, 476 U.S. 207, 211 (1986) (quoting Rawlings v. Kentucky, 448 U.S. 98, 105 (1980)).

142. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

143. The parties in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), raised Fourth Amendment questions unique to personal location information. For discussion of how that case affects the collection of V21 location data, see *infra* sections III(A)(3)–(4).

144. *See supra* notes 47–51 and accompanying text.

145. Longoria, *supra* note 41, at 13.

146. *Katz*, 389 U.S. at 351.

147. *See supra* notes 47–50 and accompanying text.

148. Smith v. Maryland, 442 U.S. 735, 745 (1979) (holding that a person does not have a reasonable expectation of privacy in information conveyed to a third party).

Third, the data involved in V2I is a small segment of the total data that modern vehicles regularly transmit to manufacturers.[149] Again, connected-vehicle drivers may be unaware of the scope and frequency of the data that they provide; but these technologies are far from novel. Vehicles have shipped with connected roadside-assistance platforms for at least 20 years.[150] Nor is it an unknown that vehicle data is valuable for criminal investigations: Mainstream news outlets have reported how police use both old and new connected-vehicle technologies.[151] This general knowledge, paired with the connected-vehicle driver's consensual use of a V2I system,[152] indicates that V2I data is not something that the driver "seeks to preserve as private."[153]

2. An Expectation of Privacy in V2I Telematic Data Would Be Unreasonable.—To find a search under the *Katz* test, a court also must conclude that any expectation of privacy is one "that society is prepared to recognize as 'reasonable.'"[154] This element raises the question of "whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment."[155] In other words, "[t]he reasonableness of an expectation of privacy turns on 'our "societal understanding" about what deserves "protection from government invasion."'"[156]

Once again putting location information aside,[157] it is not immediately obvious how collecting V2I telematics creates a search that violates the "societal values protected by the Fourth Amendment."[158] That is, an

149. *See supra* notes 4–10.

150. *See, e.g.*, Order to Comply with Roving Interception of Oral Communications at 1–2, *In re* United States, No. 2:01-cv-01495 (D. Nev. Dec 19, 2001) (compelling an early vehicle-monitoring service to "monitor oral communications" inside a suspect's Mercedes).

151. *See* Brewster, *supra* note 121 (describing how police have served connected-vehicle companies with warrants for data since at least 2001); Julia Love, *supra* note 91 (reporting on the use of autonomous-vehicle footage in police investigations); Aaron Gordon, *San Francisco Police Are Using Driverless Cars as Mobile Surveillance Cameras*, VICE (May 11, 2022, 9:00 AM), https://www.vice.com/en/article/v7dw8x/san-francisco-police-are-using-driverless-cars-as-mobile-surveillance-cameras [https://perma.cc/DX9E-J3NP] (describing the same techniques on a popular news site).

152. But consider that "consensual use" may not be so clear-cut. Maybe a driver could opt out of providing V2I communications. But if doing so means he also foregoes substantial safety benefits, is his continued use truly consensual? *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (noting that cellular location information "is not truly 'shared' as one normally understands the term" because cell phones are "indispensable to participation in modern society").

153. *Cf.* Katz v. United States, 389 U.S. 347, 351–52 (1967) ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

154. *Id*. at 361 (Harlan, J., concurring).

155. Oliver v. United States, 466 U.S. 170, 182–83 (1984).

156. United States v. Turner, 839 F.3d 429, 435 (5th Cir. 2016) (quoting United States v. Smith, 978 F.2d 171, 177 (5th Cir. 1992)).

157. *See infra* sections III(A)(3)–(4).

158. *Oliver*, 466 U.S. at 183.

expectation of privacy in telematic vehicle information is probably not objectionably reasonable. This conclusion stems from the fact that all the data sent out in the V2I basic message reflects the plainly visible state of the car. Thus, the information that the transmissions convey is "knowingly expose[d] to the public."[159] This is particularly true when the vehicle is traveling along a public roadway.[160]

In other words, the information in V2I communications (speed, heading, brake and transmission status, steering wheel angle, etc.) can all be determined not only by reading the vehicle's basic messages,[161] but also by simply looking at the vehicle itself. An observer can observe brake status by looking at the vehicle's brake lights. He can view transmission status by looking at the back of the car.[162] And he can infer the angle of the steering wheel by looking at the angle of the front wheels. In sum, the information contained in a V2I basic message is the same information that is readily apparent to the naked eye.[163] The Supreme Court has "not deviated from the understanding that mere visual observation does not constitute a search."[164] This suggests that an expectation of privacy in V2I telematic information would not be objectionably reasonable.

Moreover, the driver knowingly accepts a service through V2I communications. He receives safety alerts from the city's stoplight or clearance warnings from the state's overpass. Even if he does not know the specifics, he must understand that this requires that his vehicle supply some

159. *Katz*, 389 U.S. at 351.

160. *See* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). *But see* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere."). The implications of *Carpenter* complicate this analysis. *See infra* sections III(A)(3)–(4).

161. For the information contained in basic messages, see *supra* notes 51–63.

162. Modern cars are required to have lights on the rear of the car that display when the transmission is in reverse. 49 CFR § 571.108 (2023) (defining federal requirements for vehicle lighting, including "backup lamps").

163. This fact separately bolsters the conclusion that connected-vehicle drivers do not exhibit a subjective expectation of privacy. As a California appellate court stated, a driver cannot show "a subjective expectation of privacy in [her vehicle's speed and braking] because she was driving on the public roadway, and others could observe her vehicle's movements, braking, and speed, either directly or through the use of technology . . . ." People v. Diaz, 153 Cal. 3d 90, 102–03 (Cal. Ct. App. 2013). Instead, the "technology merely captured information defendant knowingly exposed to the public." *Id.* at 103.

164. United States v. Jones, 565 U.S. 400, 412 (2012). *But see* Kyllo v. United States, 533 U.S. 27, 34 (2001) ("[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . constitutes a search—at least where (as here) the technology in question is not in general public use." (quoting Silverman v. United States, 365 U.S. 505, 512 (1961))).

information. It is probably not reasonable for a driver to receive those services and at the same time think his communications remain private.

However, a court has room to disagree. Even if a driver knowingly exposes his vehicle on a roadway, he does not expect that its information is so easily accessible at such a high degree of precision as permitted by a V2I system. Practically, even if a driver knows that anyone could see his car driving through an intersection, he does not expect that his precise speed is transmitted ten times a second.[165] It is thus the *precision* of V2I data, not the characteristics that it describes, that most strongly suggests that an expectation of privacy in it is reasonable.

But even if it appears a court could decide this element either way, tipping the scales is the Supreme Court's repeated holding that people have a "diminished expectation of privacy in an automobile."[166] Its conclusion rests on the fact that, as mentioned, a "car has little capacity for escaping public scrutiny" while traveling on public roads.[167] The Court has also noted that vehicles are subject to "pervasive schemes of regulation, which necessarily lead to reduced expectations of privacy."[168] Connected-vehicles are no less subject to regulation. In fact, their ability to collaborate with infrastructure through V2I communications necessarily requires more regulation than a vehicle that is not "smart." It follows then that a court is unlikely to find that a driver's expectation of privacy regarding his vehicle's V2I telematic data is "objectively reasonable."

To this point, Fourth Amendment law appears to suggest that the government would not be conducting a search by collecting V2I telematic data.[169] Put another way, the government probably would not be violating connected-vehicle drivers' reasonable expectation of privacy. In 2018, however, the Court decided a landmark case in *Carpenter v. United States*.[170]

165. *See* subpart I(B) (describing the V2I basic message format).

166. *E.g.*, United States v. Knotts, 460 U.S. 276, 281 (1983).

167. Cardwell v. Lewis, 417 U.S. 583, 590 (1974).

168. California v. Carney, 471 U.S. 386, 392 (1985).

169. The law may apply differently if the government goes beyond *mere collection* to also require that drivers *transmit* V2I data. Under those circumstances, *City of Los Angeles v. Patel*, 576 U.S. 409 (2015), is instructive. That case dealt with a city ordinance that required that hotels (1) keep records on guests and (2) disclose those records to police without warrant. *Id.* at 412. The Court struck down the ordinance after concluding that the second requirement imposed a Fourth Amendment search. *Id.* at 428. However, the Court took no issue with the first requirement. *Id.* at 423 ("[N]othing in our opinion calls into question those parts of [the ordinance] that require hotel operators to maintain guest registries containing certain information."). The Department of Transportation's proposed rule, FMVSS-150, only mandates manufacturers ship vehicles with the hardware for connected-vehicle communications. The rule stops short of expressly mandating that drivers use that hardware to transmit V2I information. *See supra* notes 87–89 and accompanying text. So, it appears to impose the first requirement at issue in *Patel* but not the second. But if a future policy does take the additional step of requiring that drivers transmit their data, the circumstances would more closely resemble *Patel* and thus suggest that a transmission mandate is a search.

170. 138 S. Ct. 2206 (2018).

While its effects are unsettled, the Court's reasoning in *Carpenter* suggests that collecting V2I messages, *to the extent that they reveal location information*, may still violate drivers' Fourth Amendment rights.

3. Carpenter *Raises Questions About Collecting V2I Location Information*.—*Carpenter* suggests that collection of *location information* contained in V2I communications may still be a Fourth Amendment search.[171] The Court in *Carpenter* asked whether the government violated the Fourth Amendment when it failed to secure a warrant before obtaining "wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls."[172] Police had secured two court orders under a federal statute[173] allowing them to access 127 days of information and "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[174] Confronted with this, the Court had to "address[] a person's expectation of privacy in his physical location and movements."[175]

The Court held that this acquisition of location information through Carpenter's cell-service provider was a Fourth Amendment search.[176] The Court decided this "[i]n light of the deeply revealing nature of [cellular location information], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[177] While the acquisition of the information through Carpenter's cell-service provider was a prominent feature of this case,[178] the Court specifically noted that it does not matter if

171. *Carpenter* dealt with location information. *See id.* at 2211 (discussing how when cell phones connect to cell sites, they "generate a time-stamped record known as cell-site location information"). It does not speak to the lawfulness of collecting telematic information, such as vehicle speed and heading. *See generally id.* (reviewing the constitutionality of the government collecting cell phone records and location information).

172. *Id.* at 2214.

173. Stored Communications Act, 18 U.S.C. § 2703(d) (allowing for the acquisition of electronic records based on "specific and articulable facts showing that there are reasonable grounds to believe" that the records "are relevant and material to an ongoing criminal investigation"). The standard for a § 2703(d) order "falls well short of the probable cause required for a warrant." *Carpenter*, 138 S. Ct. at 2221.

174. *Carpenter*, 138 S. Ct. at 2212.

175. *Id.* at 2215.

176. *Id.* at 2223.

177. *Id.*

178. The Government advanced an argument in *Carpenter* using the "third-party doctrine." *See id.* at 2219–20 (explaining that the case comes down to requesting cell phone records from a third party). That doctrine states that individuals do not have a reasonable expectation of privacy in the information that they voluntarily convey to another. *See* Smith v. Maryland, 442 U.S. 735, 743–46 (1979) (holding that installation of a pen register is not a Fourth Amendment search); United States v. Miller, 425 U.S. 435, 443 (1976) (holding that the government did not violate the Fourth Amendment when it warrantlessly obtained bank records). The Court curtailed the third-party doctrine in *Carpenter* by concluding that the acquisition of cellular location information was a search. *Carpenter*, 138 S. Ct. at 2223.

"the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier."[179] Either way, "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cellular location information]."[180]

Carpenter suggests that collecting drivers' V2I location information would be a search. There are many similarities between the two technologies and the information they collect. First, cellular location information and V2I communications are "effortlessly compiled" by "automatic" systems.[181] Second, both reveal the location of individuals, and even more so in "compact coverage areas, especially in urban areas" where the density of equipment is higher.[182] Third, both are collected for "business purposes"—cellular location information for "finding weak spots in their network and applying 'roaming' charges"[183] and V2I location information for traffic safety and planning.[184] And fourth, both have a "retrospective quality."[185] That is, both cellular and V2I location information, once compiled, allow an investigator to "travel back in time to retrace a person's whereabouts."[186]

Fifth, finally, and most importantly, both cellular and V2I location information raise the same policy concerns underpinning the Fourth Amendment. As the Court expounded in *Carpenter*, the Fourth Amendment "seeks to secure 'the privacies of life' against 'arbitrary power.'. . . [and] 'to place obstacles in the way of a too permeating police surveillance.'"[187] Regardless of whether it comes from cell towers or stoplights, accurate and "all-encompassing" location information "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[188] In *Carpenter*, the Court extended Fourth Amendment protections to cellular location information based on the ability of this information to reveal intimate details of private lives.[189]

179. *Carpenter*, 138 S. Ct. at 2217.

180. *Id.*

181. *Id*. at 2216, 2223.

182. *Id.* at 2211–12 (noting that higher density of cellular towers allows phone carriers to generate more accurate location information). Like a cellular network, a V2I network is better able to capture connected-vehicle locations given more nodes in the system.

183. *Id.* at 2212.

184. *See supra* notes 30–34 and accompanying text.

185. *Carpenter*, 138 S. Ct. at 2218.

186. *Id.*

187. *Id.* at 2214 (first quoting Boyd v. United States, 116 U.S. 616, 630 (1886); and then quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

188. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

189. *Id*. at 2223.

In doing so, the Court acted on its historical uneasiness with how location information fits into the *Katz* framework.[190] As Justice Sotomayor wrote just six years before *Carpenter*, electronic location surveillance, such as "GPS monitoring[,] is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously."[191] Thus, "it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[192] She also noted that "[w]ith increasing regularity, the government will be capable of duplicating the monitoring undertaken in [*Jones*] by enlisting factory- or owner-installed vehicle tracking devices."[193] Connected vehicles may prove Justice Sotomayor prescient.

4. But Cellular and V2I Location Information Differ Qualitatively and Quantitatively.—With a closer look, it is not so clear that *Carpenter* applies to the location information that the government will collect through smart infrastructure. This is because cellular location information and the location information in V2I communications "differ in both a quantitative and a qualitative sense."[194]

Quantitatively, V2I collects far less information. Consider first that V2I collection is geographically limited. The technology relies on government-owned infrastructure to collect connected-vehicle data. Smart infrastructure can only capture connected-vehicle locations along roads in their immediate vicinity.[195] By contrast, "[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[196]

V2I collection is also temporally limited. Smart infrastructure only collects a driver's location when they are a driver. This means that V2I communications, unlike cell networks, do not allow for the "twenty-four hour surveillance" at issue in *Carpenter*.[197] Collecting data only during a person's

190. *See*, *e.g.*, United States v. Jones, 565 U.S. 400, 412 (2012) ("It may be that achieving [four weeks of electronic GPS surveillance] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy . . . ."); *id.* at 430 (Alito, J., concurring in the judgment) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."); *id.* at 415 (Sotomayor, J., concurring) ("I agree with Justice Alito [on the impact of GPS monitoring on expectations of privacy].").

191. *Id*. at 415–16.

192. *Id.* at 416 (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

193. *Id*. at 415.

194. *See* Riley v. California, 573 U.S. 373, 393 (2014) (holding that police cannot warrantlessly search cell phones incident to an arrest because of the quantity and quality of data that cell phones contain).

195. *See* HARDING ET AL., *supra* note 18, at 26 (noting that connected vehicle will broadcast their basic message to receivers within 300 meters).

196. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

197. *Id*. at 2215.

time driving on public roadways does not yield the same "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[198] Rather, those communications only reveal information about a "discrete 'automotive journey,'" something the Court previously said was beyond Fourth Amendment protection.[199] Put simply, the amount of location data that V2I yields is far less "comprehensive" than the location information revealed through cell phones.[200]

Additionally, V2I data is qualitatively inferior because it is not as "detailed" or "encyclopedic" as cellular information.[201] In *Carpenter*, the government only had to provide the cellular companies with the name of the defendant to receive 12,898 location points in return.[202] The request was simple because the data was readily tied to a single user. But an officer seeking to learn a suspect's location using V2I communications must do far more. Ascribing connected-vehicle messages to a particular driver requires not only technical expertise but also a chain of inferences.[203] The data is anonymous; it must be deanonymized to be useful. Granted, this process is not arduous (and it is easier given complementary data).[204] But it is not as easy for the government as submitting a request to the phone company.

Indeed, this distinction in the quality and quantity of cellular and vehicle-based location information is one that the Court itself alluded to in *Carpenter*. When discussing *Jones*, Chief Justice John Roberts wrote that "historical cell-site records present even greater privacy concerns than the [location] monitoring of a vehicle."[205] He also noted for the majority that the holding of *Carpenter* was a "narrow one" that did not directly speak to "other business records that might incidentally reveal location information."[206] Collected V2I communications likely fall into this category of "other

198. *Id.* at 2220.

199. *Id.* at 2215 (quoting United States v. Knotts, 460 U.S. 276, 285 (1983) (Brennan, J., concurring)). The Court relied on the fact that *Carpenter* dealt with comprehensive, "twenty-four hour surveillance" when distinguishing it from the electronic surveillance of a "discrete automotive journey" at issue in *Knotts. Knotts*, 460 U.S. at 278–79 (majority opinion). *Knotts* dealt with electronically tracking a suspect through a beeper that captured location information along public roads for a few hours. *Id.* at 278. The Court held that the technique in *Knotts* was not a search. *Id.* at 285.

200. *See Carpenter*, 138 S. Ct. at 2217 (noting that cellular location data provides a "comprehensive record of the person's movements").

201. *Id.* at 2216.

202. *Id.* at 2212.

203. For an explanation of how law enforcement can use V2I data, see *supra* subpart II(B).

204. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1154, 1157 (2002) (describing the "aggregation problem" that presents when the government has access to facts that "may seem innocuous but when combined, they become more telling").

205. *Carpenter*, 138 S. Ct. at 2218.

206. *Id.* at 2220.

business records," especially considering that they only reveal location circumstantially. Add this to the fact that V2I location information is quantitatively and qualitatively inferior to the data in *Carpenter*, and the result is that *Carpenter* does not conclusively indicate that collecting V2I location information is a Fourth Amendment search.

B. Even if It Is a Search, V2I Data Collection Is Reasonable Under the "Special Needs" Doctrine

Even assuming that collecting drivers' V2I communications is a Fourth Amendment search, it is likely reasonable and thus constitutional. This is because of a series of Supreme Court cases that permit searches without warrant or individualized suspicion under the "special needs" doctrine.

1. "Special Needs" Justify a Search Without Warrant or Suspicion.— Given a Fourth Amendment search, a court assesses whether that search was reasonable.[207] The restraint of reasonableness "generally bars officials from undertaking a search . . . absent individualized suspicion [of wrongdoing]. Searches conducted without grounds for suspicion of particular individuals have been upheld, however, in 'certain limited circumstances.'"[208] One of those circumstances is the existence of "special needs, beyond the normal need for law enforcement."[209] Identifying whether special needs justify a search requires a court to balance "the promotion of legitimate governmental interests" against "the degree to which [the search] intrudes upon an individual's privacy."[210] A "general interest in crime control" will not "suspend the usual requirement of individualized suspicion."[211]

Neither individualized suspicion nor a warrant is necessary if a search is unintrusive and supportive of a compelling public need.[212] In *Skinner v. Railway Labor Executives' Association*, the Court assessed whether the

207. *See* United States v. Sharpe, 470 U.S. 675, 682 (1985) ("The Fourth Amendment is not, of course, a guarantee against *all* searches and seizures, but only against *unreasonable* searches and seizures.").

208. Chandler v. Miller, 520 U.S. 305, 308 (1997) (quoting Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989)); *see also* Maryland v. King, 569 U.S. 435, 447 (2013) ("In giving content to the inquiry whether an intrusion is reasonable, the Court has preferred 'some quantum of individualized suspicion . . . [as] a prerequisite to a constitutional search or seizure. But the Fourth Amendment imposes no irreducible requirement of such suspicion.'" (alteration in original) (quoting United States v. Martinez-Fuerte, 428 U.S. 543, 560–61 (1976) (citation omitted))).

209. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 619 (1989) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)).

210. Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

211. City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) (quoting Delaware v. Prouse, 440 U.S. 648, 659 n.18 (1979)).

212. *See Skinner*, 489 U.S. at 634 (holding that toxicological tests to determine the fitness of railroad employees did not need a warrant due to the "diminished expectation of privacy" and "surpassing safety interests").

Federal Railroad Administration (FRA) violated railway employees' Fourth Amendment rights by requiring them to take drug and alcohol tests.[213] The FRA had acted through the federal rulemaking process to enact "regulations that mandate[d] blood and urine tests of employees who [were] involved in certain train accidents"—a search that the Court noted was "minimal" and "limited."[214] The FRA took this step in response to a "significant problem" related to drug and alcohol abuse that created "obvious safety hazards."[215] In the eleven-year period preceding the rule's enactment, substance-related railroad accidents had cost $19 million and forty-two lives.[216]

The Court upheld the FRA's policy as a reasonable search given its "special need[]" in "ensuring the safety of the traveling public."[217] The Court relied on "the limited discretion exercised by the railroad employers under the regulations, the surpassing safety interests served by toxicological tests in this context, and the diminished expectation of privacy that attaches to information pertaining to the fitness of covered employees."[218] This last point (employees' diminished expectation of privacy) stemmed from "their participation in an industry that is regulated pervasively to ensure safety."[219]

The Court reaffirmed its holding in *Skinner* only a year later.[220] In *Michigan Department of State Police v. Sitz*, the Court assessed a state program establishing drunk-driving checkpoints.[221] "All vehicles passing through a checkpoint would be stopped and their drivers briefly examined for signs of intoxication."[222] After noting that the stops were warrantless seizures under the Fourth Amendment, the Court held that they were nonetheless reasonable.[223] In balancing the state's interest against its intrusion on drivers' privacy, the Court reasoned that "the magnitude of the drunken driving problem [and] the States' interest in eradicating it" were beyond dispute.[224] "Conversely, the weight bearing on the other scale—the measure of the intrusion on motorists stopped briefly at sobriety checkpoints—[was] slight."[225]

213. *Id.* at 606.

214. *Id.* at 606, 624.

215. *Id. at* 607–08.

216. *Id.* at 607.

217. *Id.* at 619–21.

218. *Id.* at 634.

219. *Id*. at 627.

220. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990) (upholding the constitutionality of sobriety checkpoints).

221. *Id.*

222. *Id.*

223. *Id*. at 450, 455.

224. *Id.* at 451.

225. *Id.*

But the Court eventually limited the special needs exception. It held in *Ferguson v. City of Charleston*[226] that a "general interest in crime control" will not justify a "special needs" search.[227] That case considered a program at a state-run hospital that tested pregnant mothers for narcotics use.[228] The hospital was "concerned about an apparent increase in the use of cocaine by" prenatal patients, so it contacted the police to offer its "cooperation in prosecuting mothers whose children tested positive for drugs at birth."[229] The hospital intended to use the threat of prosecution to deter mothers from drug abuse, and "prosecutors and police were extensively involved in the day-to-day administration of the [testing] policy."[230] In holding that the special needs doctrine did not apply, the Court relied heavily on the fact that the searches were "designed to obtain evidence of criminal conduct."[231]

2. Traffic Safety Is a "Special Need" Permitting V2I Collection.— Assuming that the government's collection of V2I communications is a Fourth Amendment search,[232] the special needs doctrine suggests that it may require neither warrant nor individualized suspicion. Consider first that collecting V2I communications, like compelling drug and alcohol tests in *Skinner*, is minimally intrusive and done in response to a compelling need for traffic safety. *Skinner* dealt with a federal rule mandating drug and alcohol tests of all railway employees involved in accidents.[233] If the bulk collection of drivers' V2I data is indeed a search, it may likewise be enabled by a Department of Transportation regulation.[234] The Department enacted the rule in *Skinner* in response to the "significant problem" of substance abuse in rail workers.[235] The Department cited as support the fact that substance-related accidents caused forty-two deaths over the eleven-year period preceding the rule's adoption.[236] With V2I, the Department seeks to implement the technology to usher in "a new era of traffic safety,"[237] citing as support tens

226. 532 U.S. 67 (2001).

227. *See id.* at 81, 86 (concluding that "[t]he Fourth Amendment's general prohibition against nonconsensual, warrantless, and suspicionless searches necessarily applies").

228. *Id.* at 70.

229. *Id.* at 70–71.

230. *Id.* at 72, 82 (discussing the threat of prosecution as critical to "the program's success in getting women into treatment and keeping them there").

231. *Id.* at 86.

232. Mere collection of V2I communications is probably not a search. *See supra* subpart III(A). But this section proceeds with the assumption that collection alone rises to a Fourth Amendment search. It asks how the special needs doctrine applies to that assumed search.

233. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 606 (1989).

234. For an explanation of FMVSS-150, see *supra* notes 87–89 and accompanying text.

235. *Skinner*, 489 U.S. at 607.

236. *Id.*

237. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., FMVSS NO. 150 VEHICLE-TO-VEHICLE COMMUNICATION TECHNOLOGY FOR LIGHT VEHICLES, at E-3 (2016),

of thousands of annual, vehicle-related fatalities.[238] The *Skinner* rule requiring urine and blood tests was also far more intrusive on the individual than V2I communications would be—drivers may not even know that infrastructure is collecting their data.[239]

Finally, both the employees in *Skinner* and drivers on public roads have diminished expectations of privacy—the employees by nature of "their participation in an industry that is regulated pervasively to ensure safety."[240] Similarly, the Court has noted that drivers have a diminished expectation of privacy because cars are heavily regulated.[241] The Court in *Skinner* dispensed with the need for a warrant and individualized suspicion because of "surpassing safety interests," "diminished expectation[s] of privacy," and what it felt was a "minimal" intrusion.[242] A court applying this reasoning would likely find that V2I collection is similarly excepted from those requirements given the government's interest in traffic safety, drivers' diminished expectation of privacy, and the unintrusive nature of collection.

Analogizing *Sitz* supports this conclusion. That case established that drunk-driving checkpoints did not violate the Fourth Amendment.[243] Those checkpoints stopped all drivers in response to a compelling problem with drunk driving.[244] With V2I, all connected-vehicle drivers (and eventually all drivers) will submit their information to smart infrastructure because the technology will improve traffic safety. The *Sitz* Court concluded that the sobriety checkpoints were minimally intrusive based on the "duration of the seizure and the intensity of the investigation" and thus did not cause any subjective concerns.[245]

Appling these same two factors, collecting V2I data is probably similarly unintrusive. Because transmission occurs in the background without the user's involvement, connected-vehicle drivers are not seized as they are during a traffic stop.[246] There is no "seizure" of which to measure the duration. But on the other hand, a court could consider the "investigation"

---

https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/v2v_pria_12-12-16_clean.pdf [https://perma.cc/92FT-T9PT].

238. *Id.*

239. *Compare Skinner*, 489 U.S. at 609 (describing how authorities would transport employees to the hospital and draw their blood following an accident), *with* Glancy, *supra* note 45, at 1656 ("The operation of [connected-vehicle] technology will be invisible to a vehicle driver.").

240. *Skinner*, 489 U.S. at 627.

241. California v. Carney, 471 U.S. 386, 392 (1985) ("The public is fully aware that it is accorded less privacy in its automobiles because of this compelling governmental need for regulation."); *see also supra* sections III(A)(2)–(3).

242. *Skinner*, 489 U.S. at 624, 634.

243. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

244. *Id.* at 447, 451.

245. *Id.* at 452.

246. Glancy, *supra* note 45, at 1656.

involved in V2I to be substantial—the data is both granular and voluminous.[247] However, that data describes vehicle characteristics that are visible to the naked eye, even if their precise values are not immediately obvious. Considering both of these factors, it is plausible that V2I is only as intrusive as the traffic stops in *Sitz*, if not less so.[248] A court would balance this against the same interest in traffic safety that propelled the *Sitz* Court. The outcome is difficult to predict, but *Sitz* suggests that mandating V2I as a search is probably reasonable.

Finally, *Ferguson* is distinguishable from V2I collection if traffic planners collect V2I data to improve traffic, not to pursue a "general interest in crime control."[249] Granted, the facts of *Ferguson* resemble what a V2I future looks like: Traffic managers could allow criminal investigators to use V2I data much like the hospital in *Ferguson* turned drug test results over to police.[250] But the purposes of collection could differ between the cases.

In *Ferguson*, the Court declined to extend the special needs doctrine to justify the searches because "the immediate objective of the searches was to generate evidence for *law enforcement purposes*."[251] A court may not find that this holding prevents the collection of V2I communications; much depends on how collection is conducted.[252] If it is clear that a city or state emplaced a V2I system with the primary purpose of assisting criminal investigations, the facts would resemble *Ferguson* and support the same conclusion.[253] But if authorities instead primarily employed V2I to improve

247. For further discussion on the characteristics of V2I communications data, see *supra* notes 51–56 and accompanying text.

248. *Cf.* United States v. Diaz-Castaneda, 494 F.3d 1146, 1151 (9th Cir. 2007) ("[A] license plate check [using a police database] is not intrusive. Unless the officer conducting the check discovers something that warrants stopping the vehicle, the driver does not even know that the check has taken place.").

249. Ferguson v. City of Charleston, 532 U.S. 67, 81 (2001) (quoting City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000)).

250. *Id.* at 71–72. There is a world of difference, however, between sharing the information of a medical patient and that of a driver. *Compare id.* at 78 ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."), *with* the discussion of a driver's reasonable expectation of privacy *supra* sections III(A)(1)–(2).

251. *Ferguson*, 532 U.S. at 83.

252. *But cf.* Jennifer Daskal & Stephen I. Vladeck, *"Incidental" Foreign Intelligence Surveillance and the Fourth Amendment*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 101, 114 (David Gray & Stephen E. Henderson eds., 2017) (arguing instead that the government's *post*-collection use of information should weigh on the reasonableness of a search authorized by Section 702 of the Foreign Intelligence Surveillance Amendments Act of 2008).

253. Circumstances indicating a primarily law-enforcement purpose are not hard to imagine. For example, a law-enforcement purpose would be obvious if traffic planners never used the collected V2I communications while police routinely used them to investigate and "were extensively involved in the day-to-day administration" of the V2I program. *See Ferguson*, 532 U.S. at 82 (discussing police involvement in a hospital's policy of drug testing patients). Similarly, if the

traffic safety—with a purely incidental investigative benefit—a court would likely decline to follow *Ferguson*.[254]

A primary, non-investigative purpose is also what distinguishes V2I from another hotly contested Fourth Amendment topic: pole cameras. Following *Carpenter*, some courts have held that prolonged video surveillance using a stationary recording device is a Fourth Amendment search that requires a warrant.[255] Others have disagreed.[256] Pole cameras have some similarities to smart infrastructure in that both are stationary, record incessantly, and capture vast information. But traffic engineers typically install V2I systems to promote safety and collect from the systems indiscriminately. In contrast, police emplace pole cameras to "obtain evidence of criminal conduct."[257] The decision to do so involves substantial discretion—police emplace pole cameras to gather evidence of an *individual's* criminal conduct.[258] Therefore, even if pole cameras suggest that V2I collection is a search, a V2I-based search is reasonable under the special needs doctrine in a manner that pole camera searches are not.

Admittedly, there are reasons to doubt that the special needs doctrine would permit warrantless V2I collection. Holding that V2I collection is reasonable based on the government's special needs would signal an expansion of the doctrine. It is one thing to say that special needs allow the government to set up a limited number of drunk-driving checkpoints. It is something different to say that the same general need for traffic safety permits state and local governments to incessantly collect information from every vehicle, particularly in a future where all infrastructure is "smart." In

communications were immediately siphoned into an Orwellian crime-detection algorithm, a court would probably follow *Ferguson*.

254. There is clearly ambiguity in how a future, large-scale V2I system will be deployed and subsequently used by law enforcement. This ambiguity does not just stymie predictions of its legality. It also indicates that a facial challenge to a V2I system would be very difficult for a court to evaluate. *See* City of Los Angeles v. Patel, 576 U.S. 409, 416 (2015) ("[C]laims for facial relief under the Fourth Amendment are unlikely to succeed when there is substantial ambiguity as to what conduct a statute authorizes . . . ."). This suggests that a motion to suppress could be the superior vehicle for challenging a V2I-based search.

255. *See, e.g.*, United States v. Moore-Bush, 36 F.4th 320, 321 (1st Cir. 2022) (holding that recording the curtilage of a home with a pole camera for eight months was a search); People v. Tafoya, 494 P.3d 613, 615 (Colo. 2021) (three months); Commonwealth v. Mora, 150 N.E.3d 297, 312–13 (Mass. 2020) (two months).

256. *See, e.g.*, United States v. Tuggle, 4 F.4th 505, 511, 529 (7th Cir. 2021) (holding that using pole cameras to surveil a home for eighteen months was not a Fourth Amendment search); United States v. May-Shaw, 955 F.3d 563, 569 (6th Cir. 2020) (twenty-three days).

257. *See Ferguson*, 532 U.S. at 84–86 (holding that a search conducted to collect evidence of criminal activity cannot qualify for the special needs exception).

258. *Cf.* Maryland v. King, 569 U.S. 435, 447 (2013) ("The need for a warrant is perhaps least when the search involves no discretion that could properly be limited by the 'interp[olation of] a neutral magistrate between the citizen and the law enforcement officer.'" (alteration in original) (quoting Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 667 (1989))).

other words, the scale of the intrusion into private affairs would exceed previous applications of the doctrine.[259]

Additionally, even though the government has an unquestionable interest in traffic safety, it is not yet clear whether V2I will yield the safety benefits that proponents expect. Yes, early V2I deployments have been successful.[260] But the full potential of the technology cannot be realized—and tested—until it is widely adopted.[261] Until then, there are reasons to doubt V2I's safety benefits. Thus, these benefits may not be great enough to justify the intrusion V2I facilitates.

So, there are reasons to doubt that a court will extend the special needs doctrine to V2I collection even if there is a strong argument that the doctrine applies. But collection is not the only area in which V2I faces a constitutional hurdle.

C. Querying a V2I Database for Evidence Is Not Its Own Fourth Amendment Search

To this point, this Note has only considered whether the *collection* of V2I data would be a Fourth Amendment search, and if so, whether that search is reasonable. But there is another potential Fourth Amendment challenge to V2I: Even if V2I communications are lawfully collected, there is a strong argument that the police trigger the Fourth Amendment when they "search" a V2I database for a criminal investigation. In other words, *accessing* collected V2I data may, on its own, constitute a Fourth Amendment event. If so, that query must itself be reasonable. And unlike any search that occurs with V2I collection, querying a V2I database for evidence is only motivated by an interest in crime control. Thus, the special needs doctrine would not apply to justify investigative queries if they are indeed Fourth Amendment searches.

1. Hasbajrami *Suggests that a V2I Database Query Would Be a Fourth Amendment Search.*—But is a database query a Fourth Amendment search? At least one prominent court has said that it can be. In *United States v.*

259. But compare V2I collection to the scale of Transportation Security Agency airport screenings. These are the closest analogous searches that (1) courts have held is reasonable and (2) approaches the scale of widespread V2I data collection. *See, e.g.*, Corbett v. Transp. Sec. Admin., 767 F.3d 1171, 1180 (11th Cir. 2014) ("The scanners at airport checkpoints are a reasonable administrative search because the governmental interest in preventing terrorism outweighs the degree of intrusion on Corbett's privacy and the scanners advance that public interest."); *see also* Chandler v. Miller, 520 U.S. 305, 323 (1997) (noting in dicta that "where the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as 'reasonable'—*for example, searches now routine at airports*" (emphasis added)).

260. *See supra* subpart I(C).

261. Crane et al., *supra* note 8, at 238 ("[I]n order to provide significant crash avoidance benefits, a connected-vehicle system requires a critical mass of connected vehicles on the road.").

Hasbajrami,[262] the Second Circuit took up this question in the context of Section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008.[263] That statute established a surveillance program that collects the electronic communications of non-Americans located abroad.[264] But the breadth of the program and the nature of electronic communications mean that Section 702 surveillance routinely sweeps up Americans' communications.[265] This "incidental" and "inadvertent" collection was at issue in *Hasbajrami*.[266]

The *Hasbajrami* court first considered whether the government violated an American's Fourth Amendment rights when it accidentally collected his communications under Section 702.[267] A unanimous panel held that it did not.[268] The court then considered whether the government conducted a Fourth Amendment search when it queried the Section 702 database for Hasbajrami's communications.[269] The court held that it did.[270] Specifically, the court noted that "querying [stored Section 702] data does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable."[271]

The court supported this conclusion with three points,[272] two of which strongly echoed *Carpenter*. First, the court cited how the Section 702

262. 945 F.3d 641 (2d Cir. 2019).

263. *Id.* at 649, 670.

264. Specifically, Section 702 requires that the government have reason to believe that the surveillance target is a non-U.S. person located abroad. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L No. 110-261, § 702, 122 Stat. 2436, 2438 (codified as amended at 50 U.S.C. § 1801). The term "U.S. person" includes categories of people who are not themselves American citizens but nonetheless receive Fourth Amendment protection (e.g., lawful permanent residents). *See* 50 U.S.C. § 1801(i) (defining "U.S. person"). This level of technicality is not necessary to discuss how Section 702 compares with V2I communications, so this discussion dispenses with it in favor of terms such as "non-American."

265. *See* Daskal & Vladeck, *supra* note 252, at 101 ("For technological reasons, however, such broad-based collection necessarily sweeps in hundreds of millions of U.S.-person communications—those of U.S. citizens and legal permanent residents, and others residing in the United States—which are protected by the Fourth Amendment.").

266. *Hasbajrami*, 945 F.3d at 646.

267. *Id.*

268. *Id.*

269. *Id.* at 669–70.

270. *Id.* at 670.

271. *Id.* at 670. The court ultimately remanded the case for factfinding into the reasonableness of the government's queries. *Id.* at 677. On remand, the district court found those warrantless queries unreasonable. United States v. Hasbajrami, No. 1:11-CR-623, 2025 WL 447498, at *19 (E.D.N.Y. Feb. 10, 2025). But the court declined to suppress the evidence derived from the queries based on the good-faith exception to the Fourth Amendment's exclusionary rule. *Id.* at *20.

272. *Id.* at 670 ("Our reasoning is based on three considerations."). The court then provided four considerations, but the fourth related to whether a query, when considered a search, is reasonable. *Id.* at 672–73.

program "is sweeping in its technological capacity and broad in its scope" to the point that a query of its data resembles a general warrant.[273] Second, "[t]reating querying as a Fourth Amendment event . . . provides a backstop to protect the privacy interests of United States persons."[274] In other words, applying the amendment to database queries furthers the Fourth Amendment's goal as stated in *Carpenter*: To place an "obstacle[] in the way of a too permeating police surveillance."[275]

As its third point, the *Hasbajrami* court noted case law trends and cited *Riley v. California* as support.[276] In doing so, it echoed an argument laid out in a scholarly piece published a year earlier that advocated for the position the court ultimately adopted.

> The querying process is relevant to the overarching reasonableness analysis *and* is a specific search that should be independently evaluated for Fourth Amendment compliance. This position is supported by, among other cases, the Supreme Court's 2014 decision in *Riley v. California*. In that case, the Supreme Court rejected the claim that law enforcement could engage in the warrantless search of a cell phone seized incident to arrest. Rather, the subsequent search of the cell phone was deemed a separate Fourth Amendment event that will generally require a warrant based upon probable cause.[277]

Put simply, a database, like a phone, is just a container for data. The government thus "searches" when it looks at the data inside the container.

Hasbajrami suggests that an investigative V2I database query may likewise be a Fourth Amendment search. First, consider that V2I collection may soon be "sweeping in its technological capacity and broad in its scope."[278] V2I systems collect incessantly, and a driver may struggle to avoid collection when those systems blanket tomorrow's public roads. Collection may resemble a "dragnet," and thus a query of V2I data may resemble a "general warrant."[279] Second, extending the Fourth Amendment to cover a query of V2I data may be the only constitutional obstacle available as "a backstop to protect the privacy interests of [Americans]" if collection is lawful.[280] Third, the willingness of courts to extend Fourth Amendment protections will certainly be a factor given both the intimacy and volume of

273. *Id.* at 671.

274. *Id.* at 672.

275. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, U.S. 581, 595 (1948)).

276. *Hasbajrami*, 945 F.3d at 670 ("[C]ourts have increasingly recognized the need for additional probable cause or reasonableness assessments to support a search of information or objects that the government has lawfully collected.").

277. Daskal & Vladeck, *supra* note 252, at 116 (citations omitted).

278. *See Hasbajrami*, 945 F.3d at 671 (describing Section 702 data).

279. *See id.* (describing Section 702 queries).

280. *See id.* at 672 (describing a benefit of treating querying as a Fourth Amendment event).

V2I data. Courts will be tempted to make an "equilibrium adjustment" in response to V2I's technological development.[281] A future court may judge that applying a precedent like *Riley* to V2I database queries requires no great leap.

2. Database Queries Are Not Searches Under the Bulk of Fourth Amendment Case Law.—However, applying the Fourth Amendment to a database query would signal a departure from how courts traditionally treat the practice. And there are reasons why a V2I database query does not raise the same concerns that the *Hasbajrami* court faced. Nor is it a clear factual match to *Riley*.

Consider the application of *Riley* first. That case dealt with the search of an arrestee's cell phone incident to his arrest.[282] As the *Hasbajrami* court pointed out, the Supreme Court interpreted the Fourth Amendment to mean that the police could not search the phone without a warrant—searching the phone was its own Fourth Amendment event.[283] A database is another kind of container, so it follows that searching a database may also require a warrant.

But there is a crucial difference between an arrestee's phone and a V2I database: The government owns the latter.[284] Granted, the database would be composed of information about people, but the government both produces and owns it.[285] So, extending the Fourth Amendment to cover queries of a government database is not the direct equivalent of prohibiting an officer from searching an arrestee's phone to access the arrestee's information. Instead, it is the equivalent to prohibiting an officer from searching *his own* phone to access *his own* information about the arrestee. *Riley* is therefore an imperfect match to something like a V2I database.[286]

---

281. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (describing how courts expand the scope of the Fourth Amendment in response to technological advancements that threaten privacy and liberty).

282. Riley v. California, 573 U.S. 373, 378 (2014).

283. *Id.* at 403; *see also* Daskal & Vladeck, *supra* note 252, at 116 ("[T]he subsequent search of the cell phone was deemed a separate Fourth Amendment event . . . .").

284. For further discussion of the ownership of V2I data, see *supra* notes 32–34 and accompanying text.

285. *Cf.* Patel v. City of Los Angeles, 738 F.3d 1058, 1062 (9th Cir. 2013) ("To be sure, the *guests* lack any privacy interest of their own in the hotel's records. But that is because the records belong to the hotel, not the guest, and the records contain information that the guests have voluntarily disclosed to the hotel." (citations omitted)), *aff'd*, 576 U.S. 409 (2015).

286. This conclusion could be different given different circumstances—such as if the government did not, in fact, own the database. Transportation agencies today often collect V2I data before sending it to third parties for analysis. ZMUD ET AL., *supra* note 32, at 29. If that data instead went directly to a third party, it is harder to argue that the government should be free to query it, as those facts then more closely resemble *Riley* or *Carpenter*.

A Section 702 database is also distinguishable. The Section 702 data that the *Hasbajrami* court considered was swept up accidentally. Its collection was not lawful in isolation. Rather, it was an unavoidable byproduct of a surveillance program that targeted people without Fourth Amendment protection. The court in *Hasbajrami* considered the entire program reasonable *despite* the warrantless collection of Americans' information. It is this information—collected lawfully but accidentally—which comprised the database at issue in *Hasbajrami*.[287] To twist a trite metaphor, the Section 702 database contains poisonous fruit of an un-poisoned tree.

A V2I database does not raise the same concerns. The collection that created it is likely lawful, either because that collection is not a search or because if it is, "special needs" justify it.[288] Both the source and the information it yields appear untainted. Moreover, the information is categorically different from the private communications in the Section 702 database: Any expectation of privacy in V2I data is not clearly reasonable,[289] while an expectation of privacy in communication contents is unassailable.

Finally, even though the Second Circuit in *Hasbajrami* is the most authoritative court to speak on whether Section 702 queries are a search, it is not alone. Other courts have reached the opposite conclusion.[290] Indeed, courts have almost invariably held that database queries are not Fourth Amendment searches in *other* contexts, such as motor vehicle[291] and criminal[292] records. Courts have even refused to recognize searches when

287. United States v. Hasbajrami, 945 F.3d 641, 661–64 (2d Cir. 2019).

288. *See supra* subparts III(A)–(B).

289. *See supra* section III(A)(2).

290. *See, e.g.*, Redacted, 402 F. Supp. 3d 45, 86 (FISA Ct. 2018) ("The Court has considered these authorities and declines to find that they require that querying of information lawfully acquired under Section 702 be considered a distinct Fourth Amendment event . . . ."); United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *26 (D. Or. June 24, 2014) ("Thus, subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search . . . .").

291. *See, e.g.*, United States. v. Diaz-Castaneda, 494 F.3d 1146, 1152 (9th Cir. 2007) ("We hold today only that when police officers see a license plate in plain view, and then use that plate to access additional non-private information about the car and its owner, they do not conduct a Fourth Amendment search."); Hallstein v. City of Hermosa Beach, 87 F. App'x 17, 19 (9th Cir. 2003) (holding that an officer could not have violated the plaintiff's Fourth Amendment rights by searching a DMV database, even if doing so violated state law); Potocnik v. Carlson, 9 F. Supp. 3d 981, 997 (D. Minn. 2014) ("No court has ever held that accessing a driver's-license database constitutes a search or seizure within the meaning of the Fourth Amendment."); Lisenby v. Lear, No. 5:09-cv-410, 2013 WL 3762953, at *3 (D.S.C. July 16, 2013) ("Plaintiff's expectation of privacy in the DMV records at issue is not objectively justifiable under the circumstances.").

292. *See, e.g.*, United States v. Ellison, 462 F.3d 557, 562–63 (6th Cir. 2006) (holding there is no Fourth Amendment search when an officer looks up a suspect's information in a police database); Jones v. Buckner, 963 F. Supp. 2d 1267, 1277 (N.D. Ala. 2013) (same); United States v. Cobb, No. 3:12-CR-53, 2012 WL 7150434, at *8 (E.D. Tenn. Dec. 27, 2012) ("Many courts have held that computer database searches are not subject to Fourth Amendment analysis.").

officers query databases compiled using automatic license-plate readers.[293] These databases can include billions of datapoints on vehicle location information.[294]

These cases reveal an analytical pattern. Each time a court assesses whether a database query is a Fourth Amendment search, it primarily looks at whether the party asserting the claim had a reasonable expectation of privacy in the data that comprises the database.[295] In other words, unless a person has a reasonable expectation of privacy in the information, he cannot assert that a query for it is a "search." Practically, the analysis is often subsumed into the question of whether *collection* of the information was a Fourth Amendment search. If the defendant did not have a reasonable expectation of privacy in the information, then neither the collection of that information *nor a query of the database it comprises* triggers the Fourth Amendment.

This analytical framework matches the Second Circuit's reasoning in *Hasbajrami*. There, the defendant's electronic communications were only in a government database because they were accidentally swept up by Section 702 surveillance. The defendant retained a reasonable expectation of privacy regarding his communications. Thus, querying a database of those communications was a Fourth Amendment search.

Contrast this with a database of motor vehicle records. A defendant plainly lacks a reasonable expectation of privacy in his license plate.[296] So, a query of a license plate database is not a Fourth Amendment search.[297]

A database of V2I communications lies between these two extremes. Whether a driver has a reasonable expectation of privacy in his V2I data is

293. *See, e.g.*, United States v. Brown, No. 19-CR-949, 2021 WL 4963602, at *4 (N.D. Ill. Oct. 26, 2021) ("The agents did not conduct a search under the Fourth Amendment when they queried the automatic license plate reader databases."); United States v. Toombs, 671 F. Supp. 3d 1329, 1339 (N.D. Ala. 2023) ("[The defendant] has not identified any other court which has held that law enforcement officers must obtain a search warrant to query an LPR database, and the court's own research has not yielded such a case."); United States v. Porter, No. 21-CR-00087, 2022 WL 124563, at *3 (N.D. Ill. Jan. 13, 2022) ("Law enforcement's use of the automated license plate reader database did not infringe upon [the defendant's] reasonable expectation of privacy.").

294. United States v. Yang, 958 F.3d 851, 855 (9th Cir. 2020) (noting that one privately owned database has over 6.5 billion license plate scans tied to specific GPS coordinates).

295. *See, e.g.*, *id.* at 861 (holding that the defendant did not have Fourth Amendment standing to challenge the police's query of a database to determine a vehicle's location because he did not have a reasonable expectation of privacy in that information); United States v. Muhtorov, 187 F. Supp. 3d 1240, 1256 (D. Colo. 2015) ("Accessing stored records in a database legitimately acquired is not a search in the context of the Fourth Amendment because there is no reasonable expectation of privacy in that information."), *aff'd*, 20 F.4th 558 (10th Cir. 2021).

296. *E.g.*, *Ellison*, 462 F.3d at 561 ("[A] motorist has no reasonable expectation of privacy in the information contained on his license plate under the Fourth Amendment.").

297. *Id.*

not entirely clear, but current law suggests he does not.[298] The case law tradition thus suggests that querying a database of that information would not be a Fourth Amendment search. But as the Second Circuit in *Hasbajrami* recognized, courts increasingly seek ways to apply the Fourth Amendment when police access sensitive personal information.[299] *Hasbajrami* itself may be a harbinger of future developments in Fourth Amendment jurisprudence that restrict government database queries. By the time that V2I communications proliferate, the Fourth Amendment may look very different. Police seeking to query a V2I database for criminal investigation may face courts much less receptive than those that exist today.

Conclusion

Where does this leave Americans in a future where each stoplight, overpass, and highway exit they pass sends and receives information about them? Possibly without the protection of the Fourth Amendment. Collecting drivers' V2I telematic data is not a search, although the law is less clear concerning V2I location information. But even if collection were a search, it is nonetheless reasonable given the "special need" for traffic safety. After collection is complete, querying a V2I database to obtain evidence of a crime should not trigger the Fourth Amendment on its own.

That is not to say that Americans will have to live with police retracing their trips through smart infrastructure. Congress and the states are well within their constitutional authority to enact rights beyond those guaranteed by the Fourth Amendment. California has demonstrated a willingness to legislate privacy protections for drivers in other contexts by limiting connected-vehicle manufacturers from collecting and selling footage from in-vehicle cameras.[300] It has also shown interest in addressing those manufacturer's broader data-harvesting activities as deceptive.[301] Texas recently followed suit.[302] And Michigan's state constitution enumerates

298. For discussion of whether an expectation of privacy in V21 data is reasonable, see *supra* subpart III(A).

299. *See* United States v. Hasbajrami, 945 F.3d 641, 670 (9th Cir. 2019) ("[C]ourts have increasingly recognized the need for additional probable cause or reasonableness assessments to support a search of information or objects that the government has lawfully collected.").

300. *See* In-Vehicle Cameras, 2023 Cal. Stat. 864 (providing protections against manufacturer and advertiser's use of in-vehicle cameras); *see also* S.B. 994, 2014 Reg. Sess. (Cal. 2014) (attempting to provide for vehicle-data protections).

301. *See CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies*, CAL. PRIV. PROT. AGENCY (July 21, 2023), https://cppa.ca.gov/announcements/2023/20230731.html [https://perma.cc/62CH-MKY5] (announcing an inquiry into data-privacy practices of connected-vehicle manufacturers).

302. *See* Plaintiff's Original Petition at 2, Texas v. Gen. Motors, LLC, No. 24-08-12392 (457th Dist. Ct., Montgomery County, Tex. Aug. 13, 2024), https://www.texasattorneygeneral.gov/sites/default/files/images/press/General%20Motors%20Data%20Privacy%20Petition%20Filed.pdf [https://perma.cc/EN8V-LAWB] (alleging that "[s]ince 2015, General Motors has installed

electronic communications as protected against unreasonable seizure, suggesting that police in that state may need a warrant to access V2I communications.[303]

At the federal level, Congress has already had success in providing privacy protections over modern cars' "black boxes."[304] It could reconsider bills that protect location information and a broader range of vehicle data. But at this early stage in the development of smart infrastructure, it should hesitate to go so far as to impose a warrant requirement on any police access to V2I data.[305] Transparency, rather than suppressing police use of this technology, is a wiser initial goal at the federal level.

Consider that this technology could be immensely valuable for legitimate public safety goals.[306] But at the same time, the public deserves to know when and how the government uses vehicle data, as well as if the government misuses it. Transparency would foster a robust public debate about restrictions on smart-infrastructure data use. It would better inform federal policy once the technology has fully developed, states have reacted to it in varying ways, and the factors of public safety and privacy can be properly weighed.

If such a vehicle-data law is the scalpel, comprehensive federal privacy legislation is the blunt instrument that many privacy advocates would prefer. Indeed, many in Congress continue to advocate for a federal privacy statute resembling the European General Data Protection Regulation.[307] That law

---

technology in its vehicles that it advertised as improving the safety, functionality, and operability of its vehicles" and that GM "[has] unlawfully collected, used, and sold the Driving Data it obtained through this technology").

303. MICH. CONST., art. 1, § 11 (2020) ("The person, houses, papers, possessions, electronic data, and *electronic communications* of every person shall be secure from unreasonable searches and seizures." (emphasis added)).

304. *See* Driver Privacy Act of 2015, Pub. L. No. 114-94, § 24302, 129 Stat. 1312, 1712–13 (assigning ownership of onboard event-detection recorders to vehicle owners); *see also* Gershowitz, *supra* note 36, at 1173–75 (discussing how the Driver Protection Act affects the warrant requirement as it relates to other vehicle computers).

305. *See, e.g.*, S. 3231, 117th Cong. (2021) (attempting to impose a warrant requirement for all vehicle data).

306. Police today regularly use data from automatic license plate readers on public roadways. Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations. This technology enables officers to quickly apprehend fugitives in operations that would be impossible if those officers needed a warrant. V2I could offer similar law-enforcement benefits when used responsibly. But transparency is necessary to ensure the technology is not misused.

307. *Cf.* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022) (attempting to establish a comprehensive consumer privacy regime). Besides enacting general privacy legislation, Europeans are also acting on vehicle data. Alja Poler De Zwart, *European Data Protection Board's Guidelines on Connected Vehicles: Key Takeaways*, 4 J. ROBOTICS, A.I. & L. 459, 459 (2021) ("[T]he focus of European data protection regulators is increasingly shifting toward

provides "data subject rights" like the right to restrict how your data is used and the right to have your data deleted.[308] It applies broadly and includes connected-vehicle drivers.[309] In a future with prolific V2I data collection, it could enable drivers to inspect their data in a transportation authority's V2I database and request its deletion. If Congress implements similar privacy legislation, it could provide the same protections and thus preempt a law specific to vehicle data.

For the privacy maximalist, such a broad-based legislative effort is the best way of addressing the concerns raised by smart infrastructure.[310] This is because connected-vehicle technologies are still developing, and their final form may look very different than what we have seen so far. Indeed, there are indications that the Department of Transportation has balked on mandating that manufacturers ship cars with the connected-vehicle hardware.[311] And the Federal Communications Commission recently removed restrictions on the bandwidth previously reserved for connected-vehicle communications, allowing anyone to broadcast on that frequency.[312]

But it would be a mistake to infer from these developments that smart infrastructure is not coming. V2I systems will proliferate, even if the specific mechanisms they use in the future are not the same as the ones they use today. The Department of Transportation may decide not to implement its rule, for

---

the collection and use of personal information generated by smart vehicles."). As just one example, Germany already has a law in place governing the disclosure of vehicle data to police. *See* Straßenverkehrsgesetz [StVG] [Road Traffic Act], July 28, 2021, § 37 (Ger.), https://www.gesetze-im-internet.de/stvg/__37.html [https://perma.cc/4FE7-2CSK] (establishing when vehicle data can be transmitted for prosecutorial purposes).

308. *See* Commission Regulation 2016/697, General Data Protection Regulation, 2016 O.J. (L 119) 39–47 (establishing the rights of data subjects).

309. *See generally Connected Vehicles and the GDPR*, CASSIE (Sept. 7, 2023), https://trustcassie.com/resources/blog/connected-vehicles-and-the-gdpr/ [https://perma.cc/5NJJ-CKVG] (describing the General Data Protection Regulation's application to connected-vehicle companies).

310. *Cf.* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1850–55 (2016) (arguing that an approach to the Fourth Amendment rooted in positive law has advantages in terms of clarity, predictability, and democratic accountability). The positive law approach has attracted at least one influential advocate. *See* Carpenter v. United States, 138 S. Ct. 2206, 2267–68, 2270 (2018) (Gorsuch, J., dissenting) (suggesting that the Court do away with "amorphous balancing tests" and instead use "positive law [to] help provide detailed guidance on evolving technologies without resort to judicial intuition").

311. *See* Joan Lowy, *Gov't Won't Pursue Talking Car Mandate*, ASSOCIATED PRESS (Nov. 1, 2017), https://apnews.com/9a605019eeba4ad2934741091105de42 [https://perma.cc/S76Y-3RDU] (reporting that "[t]he [first] Trump administration . . . quietly set aside" the proposed rule to require "new cars to be able to wirelessly talk to each other"). The rule's status remains unclear. *See* Nat'l Highway Traffic Safety Admin., *Rulemaking Docket: FMVSS No. 150, V2V Communications*, REGULATIONS, https://www.regulations.gov/docket/NHTSA-2016-0126 [https://perma.cc/BK2M-UHKN] (listing the rule as a "pending" action).

312. *See In re* Use of the 5.850-5.925 GHz Band, 35 FCC Rcd. 13440, 13441 (Nov. 18, 2020) (ordering "the expansion of unlicensed mid-band spectrum operations, while continuing to dedicate 30 megahertz of spectrum for [connected-vehicle] operations").

instance, not because V2I is no longer a goal, but because much of the hardware it requires is *already* in modern cars.[313] Similarly, the Federal Communications Commission's decision does not signal skepticism of V2I, but instead a recognition that technologies like 5G mobile networks make radio obsolete.[314]

Regardless of the technology that it uses, smart infrastructure will be a central feature of tomorrow's roadways. Everything today seems like it is becoming "smart." Our infrastructure is no different. Every year, we spend billions of dollars fixing it[315] and thousands of hours driving on it.[316] Tens of thousands of Americans die on it.[317] Smart infrastructure promises to fix some of these problems. So, the question is not whether we should make our infrastructure smart, but whether we are comfortable with it making the police a lot smarter.

313. *See* OTONOMO, *supra* note 4, at 8 (noting that 95% of new cars sold in the United States are connected vehicles).

314. *See* First Report and Order, Further Notice of Proposed Rulemaking, and Order of Proposed Modification, No. 19–138 (Oct. 28, 2020), https://docs.fcc.gov/public/attachments/DOC-367827A1.pdf [https://perma.cc/HP82-5CMM] (noting that "cellular vehicle to everything (C-V2X), a newer radio technology standard incompatible with [radio-based connected-vehicle communications], has gained momentum both domestically and internationally as a means of providing safety-related transportation and vehicular communications.").

315. *See* Press Release, The White House, Fact Sheet: White House Highlights Infrastructure Progress in Every Corner of the Country, Updates State-by-State Fact Sheets (Feb. 8, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/08/fact-sheet-white-house-highlights-infrastructure-progress-in-every-corner-of-the-country-updates-state-by-state-fact-sheets/ [https://perma.cc/E6R4-UT9W] (disclosing that the Biden Administration provided $200 billion for infrastructure projects during its first two years).

316. Press Release, INRIX, Congestion Costs Each American 97 hours, $1,348 a Year (Feb. 11, 2019), https://inrix.com/press-releases/scorecard-2018-us/ [https://perma.cc/H7SY-N5TZ].

317. An estimated 29,135 people died in motor vehicle crashes during the first nine months of 2024. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., EARLY ESTIMATE OF MOTOR VEHICLE TRAFFIC FATALITIES FOR THE FIRST 9 MONTHS (JANUARY–SEPTEMBER) OF 2024, at 1 (2023), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813670.