Hofstra Law Review

Volume 46 | Issue 1 Article 15

2-1-2018

Invading the Driver's Seat: Preventing Overbearing Targeted Advertising in Connected Vehicles

Brandon Amon
Maurice A. Deane School of Law at Hofstra University

Follow this and additional works at: https://scholarlycommons.law.hofstra.edu/hlr

 Part of the Science and Technology Law Commons

Recommended Citation
Amon, Brandon (2018) "Invading the Driver's Seat: Preventing Overbearing Targeted Advertising in Connected Vehicles," *Hofstra Law Review*: Vol. 46 : Iss. 1 , Article 15.
Available at: https://scholarlycommons.law.hofstra.edu/hlr/vol46/iss1/15

This document is brought to you for free and open access by Scholarly Commons at Hofstra Law. It has been accepted for inclusion in Hofstra Law Review by an authorized administrator of Scholarly Commons at Hofstra Law. For more information, please contact lawcls@hofstra.edu.

NOTE

INVADING THE DRIVER'S SEAT: PREVENTING OVERBEARING TARGETED ADVERTISING IN CONNECTED VEHICLES

I. INTRODUCTION

It is a cold, early Monday morning, mid-December. You hop into your autonomous car, drowsily set your office as the destination, and hit "Go." As your car transports you to work, you begin to approach a Starbucks. The company has paid the developers of the technology deployed by your automaker to direct the routes of cars—owned and driven by those who have "liked" its Facebook page or visited its website—past its stores. As you get closer, an advertisement appears on your car's infotainment display.[1] It alerts you that Starbucks is approaching and asks if you would like to stop in for your favorite latte. It may even offer a small discount or a chance to order ahead of time.[2] You decide that you would, and tap "Yes." Your car automatically reroutes and drives you into the parking lot to pick up your beverage. This may seem like a sci-fi movie or a scene from *The Jetsons*, but in reality, this connected vehicle technology is right on the horizon.[3] In

1. Infotainment systems are defined as "systems in automobiles that deliver entertainment and information content," possibly including "managing and playing audio content, utilizing navigation for driving, delivering rear-seat entertainment such as movies, games, social networking, etc., listening to incoming and sending outgoing SMS text messages, making phone calls, and accessing Internet-enabled or smartphone-enabled content such as traffic conditions, sports scores and weather forecasts." Vangie Beal, *In-Vehicle Infotainment (IVI)*, WEBOPEDIA, http://www.webopedia.com/TERM/I/in-vehicle-infotainment-ivi.html (last visited Nov. 15, 2017).

2. *See, e.g.*, Patrick Lin, *What if Your Autonomous Car Keeps Routing You Past Krispy Kreme?*, ATLANTIC (Jan. 22, 2014), http://www.theatlantic.com/technology/archive/2014/01/what-if-your-autonomous-car-keeps-routing-you-past-krispy-kreme/283221 (envisioning a scenario similar to the one written above and noting the fine line between convenience and invasiveness).

3. Cecilia Kang & Michael Fletcher, *As Automakers Tap Smartphone Technology, Concerns Grow About Use of Drivers' Data*, WASH. POST (Jan. 9, 2014), https://www.washingtonpost.com/business/economy/as-automakers-tap-smartphone-technology-concerns-grow-about-use-of-drivers-data/2014/01/09/91a505f2-78a0-11e3-b1c5-739e63e9c9a7_story.html?utm_term=.af70cddd1e62. In 2014, a number of deals between technology firms and automakers were announced, with the objective of bringing web-related services previously aimed at smartphones to a new fleet of web-enabled vehicles. *See id.*

Published by Scholarly Commons at Hofstra Law, 2018

fact, estimates suggest that the connected-car market is growing at a rate that is ten times faster than the overall car market.[4] Further, estimates suggest that by 2020—only a few years down the road—there will be upwards of 220 million connected cars on the road worldwide.[5]

In July 2016, multiple public interest groups petitioned the Federal Communications Commission ("FCC"), seeking an emergency stay to prevent automakers from rolling out cars equipped with emerging Vehicle-to-Vehicle ("V2V")[6] technology until the FCC creates formal cybersecurity standards.[7] A large part of this issue revolves around the potential sharing of the communication spectrum that was allocated to the automobile industry in 1999, allowing vehicles to "speak" to each other.[8] This spectrum has, up until this point, been used solely within the automobile industry; however, there is a push now from automakers to open this spectrum to unlicensed Wi-Fi users.[9] Automakers plan to use this spectrum to drastically reduce traffic, accidents, and fatalities,[10] but they are also contemplating using the spectrum for numerous other things, such as mobile payments, toll payments, finding parking locations, and chiefly, delivering mobile advertisements.[11] An example of some of these technologies can be seen in plans set forth by executives from automaker Audi, who plan to have a great deal of connected technology in the automobiles they roll out in the near

4. John Greenough, *The 'Connected Car' Is Creating a Massive New Business Opportunity for Auto, Tech, and Telecom Companies*, BUS. INSIDER (Mar. 11, 2015, 5:01 PM), http://www.businessinsider.com/connected-car-statistics-manufacturers-2015-2.

5. *Id.*

6. V2V technology

> lets cars broadcast their position, speed, steering-wheel position, brake status, and other data to other vehicles within a few hundred meters. The other cars can use such information to build a detailed picture of what's unfolding around them, revealing trouble that even the most careful and alert driver, or the best sensor system, would miss or fail to anticipate.

Will Knight, *Car-to-Car Communication: A Simple Wireless Technology Promises to Make Driving Much Safer*, MIT TECH. REV. (2015), https://www.technologyreview.com/s/534981/car-to-car-communication.

7. Lydia Beyoud, *FCC Studying Cybersecurity of Connected Vehicle Tech*, BLOOMBERG L.: COMPUTER TECH. L. REP. (July 28, 2016), https://www.bloomberglaw.com/document/X7UIMSM4000000?jcsearch=bna%2520A0J8Z3A1W2#jcite.

8. *Id.*

9. *Id.*

10. *See* Dorothy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J., 1617, 1619 (2014) (noting that in 2013 there were an estimated 4.8 billion hours wasted in traffic and 5.7 million police-reported vehicle crashes, all of which proponents of V2V technology seek to reduce).

11. Beyoud, *supra* note 7.

future.[12] In connection with their partnership with Google, Audi plans to allow drivers to speak to their infotainment system, with the ability to ask Google to check traffic along the route to their destination, make reservations at restaurants, and even send calendar invites through the Google servers to those that will be joining them for that dinner—all without needing to own a smartphone.[13] They have even gone so far as to plan to install a removable tablet, which passengers will be able to take out of the automobile's dashboard and pass around, with the ability to browse the web, watch videos, read audiobooks, and do anything else that can be done on a normal Internet-connected tablet.[14] While there are fears of the potential for hackers to gain access to this spectrum and possibly cause harm to vehicle operators,[15] there is also apprehension regarding the amount of information capable of being collected by vendors and other entities that will be able to access this spectrum.[16] The collection of this data, and targeting of consumers based on such data, may prove very useful, allowing people to better access the things they want, with a vehicle doubling as a quasi-assistant.[17] However, the line between convenience and invasion of privacy is a very fine one, and while some may enjoy this type of interaction in their daily lives, others may find it extremely invasive, overbearing, or unwanted.[18]

Almost every consumer who has used her computer, phone, or tablet to shop, or even search, for a product online has already been subjected to targeted advertising.[19] For example, one might visit a company's website and look into a product that she has interest in purchasing. Upon logging off that website and onto another one such as

12. Kang & Fletcher, *supra* note 3.

13. *Id.*

14. *Id.* The laws regarding the collection of data from connected vehicles are vague. *See id*. This has led to numerous questions, including what ways law enforcement will be able to use this data, whether hackers will be able to get into these collections of data, and how Google or other sites will be stopped from tracking drivers in hopes of selling targeted advertisements. *Id.*

15. *See Public Service Announcement, Motor Vehicles Increasingly Vulnerable to Remote Exploits*, FED. BUREAU INVESTIGATION (Mar. 17, 2016), https://www.ic3.gov/media/2016/160317.aspx (warning of the dangers of potential hacking efforts into connected vehicle systems and giving examples such as shutting down the engine, disabling brakes, and steering the car while it is traveling at very low speeds).

16. *Id.*

17. *See* Lin, *supra* note 2 (noting that in-vehicle ads could be "helpful video clips or images that educate [drivers] about products and solutions [they] truly might be interested in").

18. *See* Greenough, *supra* note 4 (estimating that of the roughly 220 million connected vehicles that are expected to be on the road by 2020, consumers will activate Internet-connected technology services in just 88 million).

19. Stephanie A. Kuhlmann, *Do Not Track Me Online: The Logistical Struggles over the Right "To Be Let Alone" Online*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 229, 235-36 (2011).

Google or Facebook, that user will almost certainly see advertisements on the page, pushing that very same product for which she had just shopped.[20] This is the result of "cookies."[21] Cookies allow companies to gather personal information including, but not limited to, names, addresses, telephone numbers, and email addresses, as well as a person's interests, which can be gathered from their browsing tendencies, products viewed and bought, and social media posts and actions.[22] Once collected, this data may be used by that company, or possibly sold to other companies or third parties called "data brokers," who collect, store, and sell consumer information.[23] The breadth of data collected and stored by these companies, collected only from Internet activity, is so immense that even social security numbers can be obtained, without the consumer ever having any idea.[24] The profile that is created on anyone who uses the Internet, which can be accessed by so many companies, is already tremendous.[25] Adding more data such as geographic data, driving patterns, oft-visited locations, music, and radio preferences to that profile will allow vendors to be even more specific and accurate in their targeting of consumers.[26] There is also the distinct possibility that with the power of this extremely expansive data, vendors will feel confident enough to pay developers to have consumers routed past their store whenever the route is comparable to other available routes,

20. *See, e.g.*, Craig Timberg, *Brokers Use 'Billions' of Data Points to Profile Americans*, WASH. POST (May 27, 2014), https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html.

21. Kuhlmann, *supra* note 19, at 235. Cookies are small files automatically sent by web servers to your computer when you visit a website. *Cookies*, NETLINGO, http://www.netlingo.com/word/cookies.php (last visited Nov. 15, 2017). They are stored as text files on a computer's hard drive, and can be accessed by web servers when websites are revisited. *Id.*

22. *See* Eugene E. Hutchinson, Note, *Keeping Your Personal Information Personal: Trouble for the Modern Consumer*, 43 HOFSTRA L. REV. 1151, 1153-54 (2015).

23. *Id.* at 1155.

24. Joel Stein, *Data Mining: How Companies Now Know Everything About You*, TIME (Mar. 10, 2011), http://content.time.com/time/magazine/article/0,9171,2058205,00.html. A reporter from *Time* gave his name and e-mail address to the CEO of a data broker, who was able to recite his Social Security number less than three hours later. *Id.* From other websites, the reporter was able to find what his online profile believed to be his age, interests, level of education, income, location, and marital status. *Id.*

25. *See id.* (examining the sheer depth and accuracy of information gathered and stored by numerous websites).

26. *See* Kang & Fletcher, *supra* note 3. Consumer advocate Jeffrey Chester believes that the focus of modern day advertising is to get "hyper-local data to target consumers on a much more invasive level." *Id.*

creating the scenario discussed at the beginning of this Note[27] and by other concerned advocates.[28]

Part II of this Note introduces and provides background about the various technologies emerging within the automobile industry, focusing specifically on those that are connected vehicle technologies.[29] It also examines electronic data collection on a macro level, focusing on rights to privacy and current consumer protections.[30] Part III delves into the legal issue that arises out of the intersection between technologies emerging in the auto industry, data collection, and targeted advertising in the connected vehicle arena.[31] Finally, Part IV introduces a novel solution to this issue, which is aimed at protecting the privacy rights of consumers, allowing for total control over data collected from them, and for advertisements delivered to them in their vehicles.[32] The alternatives proposed in Part IV also aim to ensure that this technology, which can and should be extremely useful in creating a safer, faster, and more convenient traveling experience, does not get abused by vendors and become a nuisance that is unwanted by the average consumer.[33]

II. DATA DRIVE: EMERGING AUTOMOBILE TECHNOLOGIES AND DATA COLLECTION IN A CONNECTED WORLD

As technology continues to advance in the modern age, vehicles are becoming smarter and more sophisticated machines, capable of interacting with each other and with the Internet.[34] At the same time, the ability for companies to track consumer behavior on the Internet has become extremely prevalent and led to the companies using and sharing this information to build extensive profiles on those consumers.[35] The

27. *See supra* note 2 and accompanying text.

28. Kang & Fletcher, *supra* note 3. Consumer advocate Jeffrey Chester envisions a day when Best Buy or McDonald's advertisements will be "served up to drivers just when they are blocks from the nearest store," and he wonders "[a]t what point does someone get a chance to make a decision not to be tracked where [she goes], and [doesn't], where [she] bank[s] and buy[s] things." *Id.*

29. *See infra* Part II.

30. *See infra* Part II.

31. *See infra* Part III.

32. *See infra* Part IV.

33. *See infra* Part IV.

34. *See* 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, 102-03 (2015) (explaining the automated and connected vehicle technologies emerging today).

35. Edith Ramirez, *The Secret Eyes Watching You Shop*, CNN, http://www.cnn.com/2014/05/30/opinion/ramirez-data-brokers-ftc (last updated May 30, 2014, 10:35 AM) ("Data brokers scoop up the digital breadcrumbs we leave as we shop in stores and

rapid advancement of both these technologies puts them on a path toward inevitable interaction, where vendors will be able to track and target drivers in their connected vehicles.[36]

A. Connected Vehicle Technology

In order for vehicles to communicate, connect, and eventually become more automated, automakers have been studying and developing "connected vehicle solutions."[37] Connected vehicle solutions "use wireless technologies to communicate in real time from . . . [V2V] and from Vehicle-to-Infrastructure . . . and vice versa."[38] These V2V and Vehicle-to-Infrastructure ("V2I") communications serve multiple purposes, but their main benefit is safety.[39] In fact, the U.S. Department of Transportation has estimated that as many as eighty percent of accidents, not including those where the driver is impaired, could be prevented or mitigated by connected vehicle technologies.[40] Both V2V and V2I communications deploy complex technologies in order to allow vehicles and their drivers to be better prepared and better protected while on the road.[41]

In addition to these "Connected Vehicle Safety Systems," there has also been tremendous growth in a set of applications designed to enhance vehicle efficiency.[42] These technologies are called "Connected Vehicle Mobility Applications."[43] This set of technologies is much broader and more homogenous than connected vehicle safety technologies, but offers a number of potential uses and benefits beyond those provided by the former.[44] The applications will generally use the

online, and apply 'big data' analytical tools to predict where we're going, what we'll buy, and what we'll do—sometimes even before we know ourselves what we'll buy next.").

36. *See* Loren Hillberg, *Why the Connected Car Will Surpass All Other IoT Initiatives (and Four Opportunities for Advertisers)*, ADAGE (Sept. 24, 2015), http://adage.com/article/digitalnext/connected-car-dwarfs-iot-initiatives/300517.

37. *See* Kohler & Colbert-Taylor, *supra* note 34, at 103.

38. KPMG & CTR. FOR AUTOMATIVE RES., SELF-DRIVING CARS: THE NEXT REVOLUTION 12 (2012), https://assets.kpmg.com/content/dam/kpmg/pdf/2015/07/self-driving-cars-next-revolution.pdf.

39. Kohler & Colbert-Taylor, *supra* note 34, at 108-09; *see* Glancy, *supra* note 10, at 1626-29 (describing V2V and V2I technologies as "connected vehicle safety systems," which many hope will soon be requirements on new vehicles, with an aim at "enable[ing] future vehicles to share the road with greater safety and efficiency").

40. KPMG & CTR. FOR AUTOMATIVE RES., *supra* note 38, at 12.

41. *See* Glancy, *supra* note 10, at 1627-35 (providing an in-depth, technical discussion of the development and purpose of these connected vehicle technologies).

42. *Id.* at 1621-22.

43. *Id.* at 1636.

44. *Id.*

Internet (in connected vehicles) or even cellular data (via connected smartphones) in order to transmit data to be used in monitoring vehicle status, providing navigation assistance, and for infotainment purposes.[45] It is these applications, which, as automobiles continue to become more connected and tech companies become more involved, will threaten the privacy of drivers' data.[46]

1. Vehicle-to-Vehicle Communications

Automobiles equipped with V2V communication technology are already deployed on roads.[47] The main purpose of V2V technology is crash avoidance.[48] The technology works via communications between nearby vehicles, which are transmitted through a communications spectrum.[49] An example of this technology at work might be a warning being provided to *Driver A* that a vehicle up ahead is braking, and therefore she should slow down, or that a vehicle hidden from the view of *Driver A* may be approaching, otherwise unexpectedly.[50] Many automakers are moving towards installing these technologies in the automobile during production, but drivers of older cars can also have one of a few different types of aftermarket V2V devices installed in their vehicles.[51]

In the late 1990s, the FCC allocated a portion of a wireless communications spectrum to the automobile industry, in order to allow for Dedicated Short Range Communications ("DSRC") between

45. *Id.* at 1628.

46. *Id.* at 1657-60.

47. *Id.* at 1628.

48. U.S. DEP'T OF TRANSP., VEHICLE-TO-VEHICLE COMMUNICATION: SAFETY PILOT MODEL TECHNICAL FACT SHEET 1 (2012), http://www.safercar.gov/staticfiles/safercar/connected/Technical_Fact_Sheet-Model_ Deployment. pdf.

49. *Id.*

50. *Id.* at 2.

51. NAT'L HIGHWAY TRAFFIC SAFETY ASS'N, U.S. DEP'T OF TRANSP., DOT HS 812 014, VEHICLE-TO-VEHICLE COMMUNICATIONS: READINESS OF V2V TECHNOLOGY FOR APPLICATION 29 (2014). "OEM," or "original equipment manufacturer" devices are those installed in the vehicle by the manufacturer during production. *Id.* These integrated systems connect to the vehicle's data bus, and can use the precise data from within the car to create safety messages. *Id.* It can also potentially allow for the car to act in a crash scenario, perhaps by tightening seatbelts. *Id.* There are also three types of aftermarket devices: "VAD," "ASD," and "RSD." *Id.* at 29-30. The "Vehicle Awareness Device" is the simplest design, and sends safety messages to other cars, but cannot provide any warnings to the driver of the vehicle it is installed in. *Id.* at 30. The "Aftermarket Safety Device" is similar to the VAD, but also has the ability to receive safety messages, and provide audio warnings to the driver. *Id.* Finally, the "Retrofit Safety Device" is the most complex aftermarket device. *Id.* It connects to the vehicle and receives information from the data bus, which allows for more sophisticated applications, and an experience similar to an OEM integrated system. *Id.* at 30-31.

vehicles.[52] The FCC dedicated 75 MHz of the spectrum at 5.850-5.923 GHz, to be used solely for these short range communications.[53] In 2003, the FCC finalized the licensing of that spectrum, and created rules as to how it could be used, and by whom.[54] DSRC technology utilizes radio waves to allow vehicles to interact with each other and with infrastructure though this spectrum.[55] They are indeed confined to short distances, with a capacity to be sent and received only from within 100 yards.[56] The FCC and U.S. Department of Transportation envisioned a dedication of this new spectrum allocation to the development of advanced crash avoidance systems and other safety applications, and connected vehicle safety systems have accomplished just that.[57]

Using omnidirectional radio signals, vehicles with V2V technology can communicate with, and "see," nearby vehicles, with a 360 degree radius of coverage.[58] This allows vehicles to rely on more than just their own sensors and provides the ability to determine the direction, speed, and operational status of surrounding vehicles—even if they are out of sight of the driver of that car.[59] Thus, operators of vehicles with V2V technology may be provided with warnings to help them avoid a number of different "crash scenarios."[60] For example, this technology, if all involved cars are equipped with it, would allow drivers to avoid rear-end collisions, potential lane-change dangers, and blind intersection collisions.[61] There are multiple safety applications that the National Highway Traffic Safety Association ("NHTSA") felt could not be replicated by any other technology in existence at the time V2V was introduced, such as left-turn assistance (warning a driver not to make a left-turn across oncoming traffic when the approaching car is traveling

52. Beyoud, *supra* note 7.

53. Glancy, *supra* note 10, at 1629.

54. Press Release, U.S. Dep't of Transp., FCC Licensing Decision Will Help Advance Safe Transportation (Dec. 17, 2003) (on file with the *Hofstra Law Review*).

55. KPMG & CTR. FOR AUTOMATIVE RES., *supra* note 38, at 12.

56. Press Release, U.S. Dep't of Transp., *supra* note 54.

57. *Id.*; *see* Glancy, *supra* note 10, at 1628-32.

58. NAT'L HIGHWAY TRAFFIC SAFETY ASS'N, *supra* note 51, at 25.

59. *Id.*

60. *Id.* at 26.

61. *Id.* at 26-28. More specifically, if a car is travelling behind another, and the front car begins to decelerate, the second car will receive a communication indicating that, and will warn the driver to brake as well. *Id.* at 28. This same sequence can apply with stopped vehicles in the path of a car, which cannot be seen by a driver because something obstructs her view. *Id.* It can also apply when a car is about to depart its lane and come into the lane of another car, or when a driver wants to change lanes to pass a slower moving vehicle, and cannot see that another car is approaching and will be in the car's path. *Id.* Finally, it can apply when two cars are approaching the same intersection, but neither driver can see the other vehicle. *Id.* at 26-27.

too quickly, or about to blow through a stop sign or red light), intersection alerts (alerting a driver that it may not be safe to enter an intersection when there is a high likelihood of a collision), and emergency electronic brake light (warning a driver if another V2V enabled vehicle is decelerating rapidly up ahead, which might not be visible to the driver due to obstructions like trucks, rain, or fog).[62] Further, V2V systems are not subject to any limitations or constraints created by weather conditions, light, or even the cleanliness of the vehicle.[63] Essentially, once enabled by most or all vehicles on the road, they will reduce accidents drastically, by warning drivers of any situation where a collision is likely to occur without some action taken by the driver to avoid it.[64]

2. Vehicle-to-Infrastructure and Vehicle-to-Everything

V2I communications technology "involves the exchange of safety and operational data between vehicles and elements of the transportation infrastructure."[65] This technology allows cars, trucks, mass transit vehicles, and emergency vehicles to interact with various elements of traffic infrastructure, such as traffic lights, which will allow for greater notice of impending danger, and thus, fewer accidents.[66]

Although V2I communications have a primary goal of preventing motor vehicle crashes, there is also an aim towards "enabling a wide range of mobility and environmental benefits."[67] The NHTSA has identified, studied, and evaluated many different types of "road side equipment" ("RSE"), which would be able to communicate with vehicles via DSRC signals.[68] During their "Safety Pilot Model Deployment," the NHTSA located the RSE around other infrastructure elements such as traffic lights and road signs, and used the RSE for applications related to signal phasing and timing, as well as approaching curves and curve speed warnings.[69] Designed to complement V2V communications, V2I communications are meant to address a number of

62. *Id.* at 25-28. Technologies available, before V2V was introduced, include vehicle-resident cameras and other sensors used to detect very nearby surroundings (for example, back-up assistance sensors). *See id.* at 26.

63. *Id.*

64. *Id.*

65. U.S. DEP'T OF TRANSP., VEHICLE-TO-INFRASTRUCTURE (V2I) PROGRAM 1 (2016), http://www.its.dot.gov/factsheets/pdf/JPO-17-442-V2I-Program.pdf.

66. *Id.*

67. NAT'L HIGHWAY TRAFFIC SAFETY ASS'N, *supra* note 51, at 32.

68. *Id.*

69. *Id.*

crash scenarios that cannot be addressed by the former, including warnings of upcoming red lights and the potential for drivers to blow through them based on their distance from the intersection and vehicle speed; warnings to drivers that they are traveling at an excess speed when approaching a curve in the road; stop sign assistance (alerting drivers not to enter a stop-sign controlled intersection when it is unsafe to do so, or that they are traveling too fast and are in danger of speeding through the stop sign); alerts to drivers when they are nearing a reduced speed zone (like a work zone) to slow down, change lanes, or brake completely; weather information and alerts about approaching hazardous conditions; railroad crossing warnings; and oversize vehicle warnings, which would be delivered to trucks exceeding height or weight limits on a certain road, alerting them to take an alternate route.[70] Further, the NHTSA included in its Safety Pilot Model Deployment some V2I communications that have the ability to interact with and alter the infrastructure itself.[71] For example, traffic signals could be set to prioritize approaching emergency vehicles by illuminating a sign to warn drivers at an intersection that an emergency vehicle is approaching, or turn lights to red to avoid a collision with an approaching emergency vehicle.[72] Once adoption of V2V and V2I technologies becomes more widespread, the goal of increased safety and reduced vehicle collisions will become more and more reachable.[73]

In addition to the automobile-centric technological applications offered by V2V and V2I communications, there are "Vehicle-to-a" ("V2X") communication applications.[74] V2X is a catch-all, which encompasses all communications between vehicles and other vehicles, infrastructure, and other systems, such as mobile devices.[75] Examples of this technology include the applications previously mentioned, but can also include vehicles interacting with their surroundings.[76] One example of this type of interaction would be an alert when public parking is available near a connected car engaging in V2X communications.[77]

70. *Id.* at 32-33.

71. *Id.* at 9.

72. *Id.*

73. *See id.* at 15 (summarizing the NHTSA's belief that "the greatest gains in highway safety in coming years will result from broad-scale application of crash avoidance technologies").

74. Glancy, *supra* note 10, at 1627.

75. *Id.*; *see* SIEMENS, VEHICLE-TO-X (V2X) COMMUNICATION TECHNOLOGY (2015), https://www.mobility.siemens.com/mobility/global/SiteCollectionDocuments/en/roadsolutions/urban /trends/siemens-vehicle-to-x-communication-technology-infographic.pdf.

76. *See* SIEMENS, *supra* note 75 (providing examples of such interactions).

77. *Id.*

These types of systems could also be utilized by motorcyclists, bicyclists, pedestrians, and those using wheelchairs or other mobility devices, allowing their presence to be detected by vehicles utilizing communications technology.[78] For example, numerous tech companies are developing smartphone applications, which will allow those who are not inside of an automobile to benefit from the increased protection provided by these technologies.[79] One such example is an initiative started by Savari, a software company who has been sponsored by the U.S. Department of Transportation, which aims to make bicyclists and pedestrians "active participants in the V2X landscape, especially in Smart City scenarios."[80] Its system would connect pedestrians and bicyclists to vehicles and infrastructure, such as traffic lights, through an application on their smartphone.[81] Using this connection, there would be warnings provided to drivers in vehicles approaching an intersection where a pedestrian, perhaps distracted, has entered the road in violation of a do-not-cross sign, or in an unmarked area.[82] Further, using the "SmartCross" phone application, pedestrians will be able to communicate with traffic signals, allowing them to request a walking phase, receive a notification when it is safe to cross, and make certain that the walking phase stays in effect until they have made it all the way across the street.[83] Beyond expanded safety applications, V2X communications will also offer drivers mobility applications, such as city information, which will provide drivers with information about their physical surroundings.[84]

3. Connected Vehicle Mobility Applications

In contrast with the numerous safety applications discussed above, Connected Vehicle Mobility Applications aim to increase convenience, information, and entertainment, by providing an "interconnected, data-rich travel environment."[85] These types of programs are available today,

78. Glancy, *supra* note 10, at 1631-32; SAVARI NETWORKS, V2X APPLICATIONS OVERVIEW (2016), http://www.savarinetworks.dreamhosters.com/wp-content/uploads/2016/05/Savari-V2PApps-DataSheet-FINALMay2016.pdf.

79. Glancy, *supra* note 10, at 1631-32.

80. SAVARI NETWORKS, *supra* note 78.

81. *Id.*

82. *Id.*

83. *Id.* In assuring that the signal does not change until the pedestrian has crossed the street fully, extra protection will be provided to those who are mobility impaired or visually impaired. *Id.*

84. *See* SIEMENS, *supra* note 75 (providing a visualization of the numerous potential V2V, V2I, and V2X applications which could be utilized on city streets).

85. CHRISTOPHER HILL, MODULE 13: CONNECTED VEHICLES (2013), http://www.pcb.its.dot.gov/eprimer/documents/module13.pdf; *see* Glancy, *supra* note 10, at 1636-

predominantly through the use of smartphones that can connect to a vehicle's infotainment system.[86] Some examples are Apple's CarPlay and Google's Android Auto.[87] Though these two applications have their slight differences, their main purposes are the same: allowing the vehicle to connect to the Internet via the driver's smartphone connectivity, and providing the ability for the driver to interact with the many applications available on her phone, right through her car's dashboard.[88] Through this interface, drivers can access a wide variety of infotainment including navigation and mapping (with traffic reports), streaming audio services, and text messaging capacity.[89] Even more impressive is the ability for these programs to provide "suggestions" to the driver based upon her prior phone use, or driving habits.[90] An illustration of this is Android Auto's "Google Now" screen, which is a contextually-aware, constantly updating stream of information about the weather, traffic and navigation data, notifications, and "shortcuts" to likely destinations that the system has created based on a driver's consistent searches and driving habits (for example, frequented locations).[91]

In addition to these "tethered" connections, which occur when a driver "plugs-in" her connected mobility device, many automakers have begun to develop "embedded" connections.[92] These connections use hardware installed in the vehicle to provide the driver with connectivity to the Internet via built-in Wi-Fi,[93] or even 4G—and soon to be 5G—modems.[94] Further, these systems will not only allow drivers to benefit from enhanced infotainment, creating a more convenient and efficient driving experience, but will also enable them to keep tabs on the status

37.

86. Glancy, *supra* note 10, at 1636.

87. Antuan Goodwin, *Android Auto vs. Apple CarPlay: Google and Apple Battle for Dashboard Dominance*, CNET: ROAD/SHOW (June 16, 2015, 9:23 PM), https://www.cnet.com/roadshow/news/android-auto-vs-apple-carplay-head-to-head.

88. Glancy, *supra* note 10, at 1636; Goodwin, *supra* note 87.

89. Goodwin, *supra* note 87.

90. *Id.*

91. *Id.*

92. *See* Andrew Meola, *Automotive Industry Trends: IoT Connected Smart Cars & Vehicles*, BUS. INSIDER (Oct. 6, 2016, 12:12 PM), http://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10.

93. *Id.*

94. Eric Jhonsa, *Connected Cars Have Potential Not Just for Chipmakers, But Won't Always Move the Needle*, THESTREET (Oct. 18, 2016, 9:30 AM), https://www.thestreet.com/story/13847339/1/connected-cars-have-potential-not-just-for-chipmakers-but-won-t-always-move-the-needle.html.

and performance of their vehicle via embedded equipment that can communicate these details to the vehicle's manufacturer.[95]

Despite all of these exciting benefits, there remains a fear, which is discussed further in Part III of this Note, that the ability for the delivery of this enhanced safety and infotainment will be accompanied by advertisements targeted at the driver and passengers "based on the type of vehicle and its location, previous content, and occupants."[96]

B. Autonomous Vehicles

In addition to connected vehicle technologies, which allow vehicles to speak to each other and infrastructure surrounding them,[97] there is also technology being developed and slowly tested on roads around the world that will allow cars to drive autonomously—with little to no human interaction.[98] This technology ranges from "selfcontained" autonomous vehicles to "interconnected" autonomous vehicles.[99] These interconnected autonomous vehicles are the ones that will interact with other vehicles and infrastructure, using the communications technologies discussed above.[100] These vehicles with autonomous or self-driving technology capabilities are beginning to be deployed, and deals have been struck between automakers, technology giants, and other companies in hopes of getting a head start on this rapidly advancing business.[101]

Although autonomous vehicles will likely be able to operate under a number of different types of designs and systems, they will all likely achieve the same result: replacing human drivers with artificial intelligence.[102] These self-driving automobiles are shaping up to take over the roads of America, with a potential fleet of trucks, buses, taxis, emergency vehicles, and most obviously, personal vehicles.[103] In order to safely and effectively travel and navigate, autonomous vehicles will

95. Glancy, *supra* note 10, at 1636-37.

96. *Id.* at 1639.

97. *See supra* Part II.A.

98. *See* Kohler & Colbert-Taylor, *supra* note 34, at 102-04 (discussing the various levels of vehicle automation).

99. Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1173-78 (2012).

100. *Id.* at 1176-77.

101. *See, e.g.*, Christopher Heine, *How the Self-Driving Car Is Turning Detroit and Silicon Valley into BFFs: GM-Lyft Deal Marks Shift in Competition*, ADWEEK.COM (Jan. 4, 2016), http://www.adweek.com/news/technology/how-self-driving-car-turning-detroit-and-silicon-valley-bffs-168824 (providing one example of such deal between General Motors and Lyft).

102. Glancy, *supra* note 99, at 1173.

103. *Id.* at 1174.

rely on and utilize a great deal of information from numerous data sources.[104] While all autonomous vehicles will be heavily data-dependent, it is how and from where that data is collected that differentiates the different types of autonomous vehicles.[105] One type of system will almost solely utilize data received from systems onboard the vehicle, and utilize downloaded maps from within the vehicle's intelligence system to navigate and travel.[106] These selfcontained autonomous vehicles would not need to communicate with any external data-points in order to carry out safe travels and thus would not send or transmit any of the data it has recoded about the status of the vehicle or its user.[107] This type of self-dependent autonomous vehicle has already been created and tested by a leader in the study of self-driving cars—Google.[108] The other type of autonomous vehicle system that is emerging places a much heavier reliance upon external sources of data and wireless communications networks.[109] These interconnected autonomous vehicles communicate with other vehicles and infrastructure, like vehicles with connected vehicle technologies discussed above, in order to receive situational information about the roadway, environment, and actions of nearby vehicles.[110] Using this and the other V2V, V2I, and V2X technologies discussed earlier, the vehicle will be able to locate and navigate itself, and be able to "speak" to surrounding vehicles and infrastructure in order to ensure the prevention of both collisions and violations of traffic laws.[111] Because of its reliance upon the sending and receiving of data over communications networks, it is possible that interconnected vehicles could be controlled and

104. *Id.*

105. *Id.* at 1173-74.

106. *Id.* at 1176-77.

107. *Id.*

108. *Id.* at 1178. The lead technician for Google's autonomous vehicle development program has stated that the "heart of [its] system" is a laser range finder which they have mounted atop the car. Erico Guizzo, *How Google's Self-Driving Car Works*, IEEE SPECTRUM (Oct. 18, 2011), http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works. This laser has the ability to generate a detailed 3D map of the vehicle's surroundings, which the vehicle then combines with high-resolution maps to produce enough data to allow the vehicle to drive itself without endangering others, contacting obstacles, or disobeying traffic laws. *Id.* In addition to the large, mounted laser range finder, the vehicle also contains other sensors such as radars mounted on the corners of the front and rear bumpers, which allow the car to "see" enough to deal with faster moving traffic; a camera on the window side of the rear-view mirror, which can see and detect upcoming traffic lights; and a "GPS, inertial measurement unit, and wheel encoder," which can pinpoint the vehicle's location and track its movements. *Id.*

109. Glancy, *supra* note 99, at 1177.

110. *Id.*

111. *Id.* at 1177-78.

operated by an outside source.[112] Although the issue of potential hacking and external control of driving is limited mainly to interconnected autonomous vehicles,[113] both of these types of systems have given rise to many concerns about the collection and privacy of personal information of the user(s) of the vehicles.[114] It is these personal information concerns that will be addressed in Part III of this Note.[115]

C. Data Collection via the Internet

Any consumer who has signed up for and posted on Twitter or Facebook, downloaded an application on a smartphone or tablet, entered a sweepstakes, subscribed to a newsletter, browsed or shopped for a product online, or even received a coupon or discount code from a store that she likes, has had pieces of information taken from her.[116] Each of these bits of information is collected, analyzed, and used to create an extensive profile, which can be utilized by companies to target consumers, or be sold or transferred to other companies for a fee.[117] Perhaps even more alarmingly, most consumers do not even know that their information is being collected, and if they do, they often do not know if, or how, they can prevent that data collection.[118]

1. A History and Explanation of Internet Data Collection and Dissemination

As mentioned earlier, cookies allow websites and companies to collect bits and pieces of information about consumers when they visit their sites.[119] Once collected, that information can be used for a variety of purposes, including building a profile on individuals—containing their social status, age, income, race, political affiliations, religion, Social Security numbers, gun-ownership records, preference in movie/music genre, and interest in health issues—and subsequently

112. *Id.* at 1177.
113. *Id.* at 1178-79.
114. *Id.* at 1178-81.
115. *See infra* Part III.
116. *See* Ramirez, *supra* note 35.
117. *See id.* ("[D]ata brokers collect billions of pieces of data on nearly every American consumer, often merging online and offline information. Data brokers are also making potentially sensitive inferences about consumers—about their health, financial status, and ethnic backgrounds."). As individual profiles are built, with an incredible amount of detail, marketers can more accurately target and display ads on the pages those specific individuals visit on the Internet. Timberg, *supra* note 20. This data can also be used by banks to ensure the identity of customers. *Id.*
118. *See* Ramirez, *supra* note 35.
119. *See* Hutchinson, *supra* note 22, at 1153-54.

predicting interests and future actions.[120] Companies can even create segments or categories of individuals based on their information:

> With potentially thousands of fields, data brokers segment consumers into dozens of categories such as "Bible Lifestyle," "Affluent Baby Boomer" or "Biker/Hell's Angels," [an FCC] report said. One category, called "Rural Everlasting," describes older people with "low educational attainment and low net worths." Another, "Urban Scramble," includes concentrations of Latinos and African Americans with low incomes. One company had a field to track buyers of "Novelty Elvis" items.[121]

The companies that are most prevalently involved in the collection of personal information online are companies called data brokers.[122] These are companies that "gather, analyze, store, and sell personal online information—which has, in turn, given rise to the data market."[123] Although consumers will essentially never have direct contact with data brokers, they are still seriously affected by the collection, manipulation, and dissemination of their data by these companies.[124] Data brokers can collect their massive database of information from numerous sources, including the government, publicly available sources of information such as social media pages, blog pages, and the rest of the Internet, and from "commercial" sources such as approved retail companies.[125] Though collection from the Internet is generally the easiest for data brokers, at this time a majority of their collected information is from these "commercial" data sources and companies.[126] Further, data brokers can obtain information regarding a person's Internet activity, such as her

120. *See* Stein, *supra* note 24; Timberg, *supra* note 20.

121. Timberg, *supra* note 20. FTC Chairman Edith Ramirez went so far as to say, "The extent of consumer profiling today means that data brokers often know as much—or even more—about us than our family and friends." *Id.*

122. *See* Hutchinson, *supra* note 22, at 1155.

123. *Id.*

124. *Id.*

125. *Id.*

126. *Id.* at 1155-56. Approved companies will often have information provided directly to them by consumers themselves. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 4 (2013), http://www.gao.gov/assets/660/658151.pdf. This occurs when consumers join loyalty or rewards card programs at stores or websites, register a product for a warranty, enter contests, or complete surveys/questionnaires. *Id.* Further, approved companies and data brokers will often enter into agreements with each other, whereby the approved company will provide the data broker with information about their customers—including purchase history, email address, and home address—in exchange for the data brokers providing them with information expanding upon current customer lists, or identifying new ones who seem to be interested in that company and its products. Hutchinson, *supra* note 22, at 1156.

IP address, which Internet browser she prefers, and her browsing habits on specific websites and the web in general.[127] One last chilling aspect of the profiles that are built on individuals is the fact that many contain their health records, which most consumers consider to be highly personal and confidential.[128]

2. Examination of Consumer Privacy Rights in America versus the European Union

While America has no enumerated right to consumer privacy,[129] other places, such as the European Union ("EU"), follow a much different path with regard to these rights.[130] The increased importance placed on individuals' privacy rights in the EU has led to greater protections and clearer policies in regard to consumer information collected online.[131]

In May 2016, lawmakers in the EU adopted agreements that drastically altered the landscape of the data collection industry.[132] The General Data Protection Regulation ("the Regulation") was created to "ensure[] that personal data can only be gathered under strict conditions and for legitimate purposes."[133] The Regulation is accompanied by a new individual privacy Directive, which is not immediately binding, but

---

127. Hutchinson, *supra* note 22, at 1155-56.

128. Kate Jennings, *How Your Doctor and Insurer Will Know Your Secrets—Even if You Never Tell Them*, BUS. INSIDER (July 9, 2014, 3:04 PM), http://www.businessinsider.com/hospitals-and-health-insurers-using-data-brokers-2014-7 ("Some hospitals and health insurers have started buying consumers' personal data in order to identify 'high-risk' patients and curtail bad health habits."). While most consumers believe that their medical records are protected by the Health Insurance Portability and Accountability Act, they generally do not realize that their health information can be inferred fairly easily based upon their credit and debit card purchases, and other sources of information (such as whether or not they have a gym membership, or whether they have an affinity for fast food). *Id.*

129. *See* Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (holding that a number of specific guarantees in the Bill of Rights create a "penumbra" of rights which do form the right to privacy under the constitution). However, the Supreme Court has not found much constitutional protection for consumer rights with relation to data collection. James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 34 (2003).

130. *See Protection of Personal Data*, EUROPEAN COMMISSION ON JUST., http://ec.europa.eu/justice/data-protection (last visited Nov. 15, 2017) (discussing regulations created and implemented in the EU in 2016, designed to reform and enhance data protection rules).

131. *See id.* ("The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business.").

132. *Id.*

133. *Digital Privacy*, EUROPEAN COMMISSION, https://ec.europa.eu/digital-single-market/en/online-privacy (last updated Aug. 17, 2017); *see also* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2017 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119/1) [hereinafter Regulation 2016/679].

must be transcribed into the laws of member countries within two years of its passing.[134] Under the Regulation, all companies need to obtain affirmative informed consent from their customers prior to collecting and processing any of their personal data.[135] Failure to comply with this requirement would result in that offending company being fined up to four percent of its annual revenue for the current year.[136] A penalty of that type would prove to be incredibly substantial to Internet mainstays with massive revenue streams, such as Google, Amazon, and Facebook.[137] In addition to the requirement of affirmative customer consent prior to data collection, the Regulation also makes data controllers (data collecting companies such as retail stores) and data processors (similar to data brokers) jointly liable in cases of data misuse or abuse.[138] This means that consumers would have a right of action against both the company that collected their data (even after giving them consent to do so) and the data processing company who utilizes that information.[139] The indirect effect of this, lawmakers hope, is that companies who intend to collect data will select the data processing company with which they will work, with much greater care and scrutiny.[140] One final aspect of the Regulation was the addition of new rules designed to make certain that any personal data breaches are reported in a quick and consistent way across the EU.[141]

A major reason for these stringent protections in the EU is the fact that Europeans have long considered privacy of personal information to be a fundamental right.[142] In fact, every European has a codified "right to respect for [] private and family life" provided by Article 8 of the

134. Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89.

135. Regulation 2016/679, *supra* note 133.

136. *Id.*

137. *See id.*

138. *Id.*

139. *See id.*

140. *Id.*

141. *Digital Privacy*, *supra* note 133. Personal data breaches refer to situations where some or all of the massive amount of personal data possessed by telecom operators or Internet service providers, which must be kept secure and confidential, is either lost, stolen, or illegally accessed. *Id.* The Directive requires that the provider reports any breach of this kind to a national authority, and informs the affected individual of any risks they face. *Id.*

142. Avner Levin & Patricia Sánchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1013 (2009).

European Convention on Human Rights.[143] Consequently, the fundamental right to privacy has been drafted into the laws of many EU member states and is recognized in the constitutions of several European nations.[144] Much of this respect for privacy derives from another key value in Europe—dignity[145]:

> Dignity is thus the theoretical basis for privacy protection in Europe. As a result, European laws are very protective of personal privacy in many areas, from consumer rights, as exemplified by the EU Directive that establishes data protection for Europeans in all their commercial transactions worldwide, to discovery in civil litigation.[146]

In this regard, European law differs substantially, at least at this time, from American law.[147] Realms of life such as credit reporting, dignity of criminal offenders, and most poignantly, data protection, are all areas where European law has "forcefully extended privacy protections to noncelebrities and nonroyals," while American law has not.[148]

III. TROUBLE AROUND THE BEND? THE INEVITABLE COLLISION BETWEEN INTERNET-CONNECTED VEHICLES AND TARGETED ADVERTISING

As personal and commercial vehicles become more technologically advanced, an entire world of possibilities, both awe-inspiring and disturbing, will open up for businesses and marketers.[149] Similar to the invention of the personal computer and the smartphone, connected vehicles will serve as a new beacon of consumer tracking and targeting.[150] The aforementioned devices have allowed companies and

143. EUROPEAN CONVENTION ON HUMAN RIGHTS art. 8 (2010), http://www.echr.coe.int/Documents/Convention_ENG.pdf; *see* Levin & Sánchez Abril, *supra* note 142, at 1014 ("There shall be no interference by a public authority with the exercise of this right [to private life] except such as is in accordance with the law.").

144. Levin & Sánchez Abril, *supra* note 142, at 1014-15.

145. *Id.* at 1015. The concept of dignity in privacy "emphasizes the development of one's personality and inner self." *Id.* at 1013. Under that thought process, "privacy encompasses the right of an individual to keep certain aspects of his life unknown to others, and thereby construct different 'situational personalities.'" *Id.*

146. *Id.* at 1015.

147. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1170-71 (2004); *see also supra* notes 129-30 and accompanying text.

148. *Id.* at 1170.

149. *See* Lin, *supra* note 2.

150. ACCENTURE, THE CONNECTED VEHICLE: VIEWING THE ROAD AHEAD (2014), https://www.accenture.com/t20160519T222110__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_4/Accenture-Mobility-Connected-Vehicle.pdf.

data brokers to build incredibly expansive profiles on all who surf the Internet.[151] Now, with the introduction of additional, previously inaccessible data points from vehicles, those profiles will become even larger and more complete.[152] With this additional data, it will become possible to direct advertisements at individuals in their cars or allow third parties—likely to be business entities—to control some of the actions of a vehicle.[153] Without some legal control over these practices, consumers and drivers in America will be faced with a huge problem; one that could potentially derail what is meant to be, and should be, a life-changing technology.[154]

A. The Profile that Data Brokers Have Already Built on Individual Consumers Is Expansive and Will Only Grow Stronger with the Information that Will Be Provided by Connected Vehicles

Earlier in this Note, an extensive discussion of data collection via the Internet and Internet-connected devices revealed just how common this behavior is, and just how much information has been collected, analyzed, and utilized in aiming specific advertisements and messages at individuals.[155] The Internet boom and subsequent smartphone craze advanced so rapidly that consumers were essentially pushed to either adapt to these new technologies or fall behind, while many still did not comprehend them.[156] In addition to the information voluntarily given by consumers—such as anything requested when signing up for an account on a website or for a newsletter—there is also data collected via cookies.[157] When an advertising content provider plants these cookies on a webpage, it can see any and all activity that one engages in on that site including what she reads, clicks on, and purchases.[158] The provider can then assemble this information, and as a result, many if not most consumers have had extensive, overarching profiles built based upon

151. *See* Ramirez, *supra* note 35.

152. Lin, *supra* note 2.

153. *Id.*

154. *See id.*

155. *See supra* Part II.C.

156. Devin Ness, Note, *Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy as We Know It*, 31 CARDOZO ARTS & ENT. L.J. 925, 928-29 (2013).

157. *Id.* at 929.

158. *Id.* The author notes that because engaging with technology is viewed as "voluntary" rather than "necessary," the information obtained via cookies is viewed as voluntarily given, just as any information that a user would knowingly input or disclose. *Id.* The author disagrees with this classification, because of the incredible reach, prevalence, and importance of modern technologies. *Id.* at 928-29.

their every move on the web.[159] Further exacerbating this issue is the emergence of social networks.[160] On these social networking websites, individuals are encouraged to share highly personal data, under the façade that it is protected under privacy policies.[161] However, the reality of these privacy policies is that they offer no true legal protection at all.[162] Finally, "cloud" services, which allow users to upload and store photos, documents, and more, often result in the collection of data as well, as many have disclaimers in their terms of service which reduce the privacy of those uploaded documents.[163] All of this data, aggregated from the numerous sources discussed above, make it a certainty that almost any web-connected individual has an extensive profile built on her, which is used to predict her next move, and to advertise directly to her on her web-enabled devices.[164]

Although all of this data provides marketers with a very full picture of individuals and their interests, there are a few important data points and sources that have been missing, most notably geographic-based data.[165] This geographic data would include driving habits and frequently visited locations—not only specific pinpoint locations, but also classes of establishments such as coffee shops or fast food restaurants.[166] This missing data is exactly the kind of information that may now become readily available with the introduction and growth of web-connected and self-driving vehicles.[167] In addition to geographic data points, marketers would now be able to collect information about the types of things a person listens to in her car, including types of music, podcasts, radio stations, news, and sports (specific leagues or teams).[168] While some of this data might have already been available for

159. *Id.* at 929; Ramirez, *supra* note 35.

160. Ness, *supra* note 156, at 929.

161. *Id.*

162. *Id.*

163. *Cloud Computing*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/cloudcomputing/##introduction (last visited Nov. 15, 2017).

164. *See* Ramirez, *supra* note 35.

165. *See* Kang & Fletcher, *supra* note 3 (discussing why data generated from a connected vehicle would surpass that currently available via smartphones and other portable devices).

166. *See* Lin, *supra* note 2 (providing an example of this, where a driver is prompted with an advertisement for Krispy Kreme as their vehicle approaches one of the chain's locations, because marketers have determined the driver is a "serial offender" when it comes to impulsive snacking based upon her driving habits and locations visited, along with her social media activity (for example, "liking" Krispy Kreme on Facebook)).

167. Kang & Fletcher, *supra* note 3; Lin, *supra* note 2.

168. *See, e.g.*, Hillberg, *supra* note 36 (discussing the numerous additional data points that will be created by connected vehicle technology, and its application with regard to radio and other in-car audio apps).

those who use music streaming services like Apple Music or Spotify, similar information would now be available for those who strictly use the radio as their in-car audio entertainment.[169] If, or when, autonomous cars take over the roads, even more data will be able to be collected via their capabilities.[170] The "drivers" of these self-driving cars will likely be able to use the infotainment system in the vehicle to browse the web, view content, shop, and do essentially anything else that they would be able to do on any of the web-connected devices we know of today.[171] This means that there will be yet another device from which data can be extracted; and based strictly upon the sheer volume of time that consumers would spend in their cars, without the burden of having to drive, it is surely plausible that much more time would be spent browsing the Internet, interacting with surroundings, and creating additional data to be consumed by marketers.[172]

With the growth of connected, and eventually autonomous, vehicles, marketers will be receiving more insight as to "real-world consumer behavior," giving them a glimpse into how the consumer spends her time, where she shops, what she eats, and to what destinations she travels.[173] This information is something that has long been craved by businesses and marketers.[174] Again, when combined with the extensive profiles that have already been built, it is essentially inevitable that connected-vehicle created data will lead to a complete destruction of consumers' basic privacy, if regulatory action is not taken.[175]

B. Targeted Advertising in Connected Vehicles Will Likely Lead to an Invasion of Consumers' Privacy Rights, Alter Daily Life, and Possibly Lead to the Demise of a Productive Technology

While increased data collection is a major problem, it is not the most pressing concern that would arise as connected vehicles continue to progress.[176] Indeed, the more frightening scenario is the inevitable invasion into those vehicles, and the numerous ways that third parties

169. *See id.*

170. Kohler & Colbert-Taylor, *supra* note 34, at 120.

171. *See supra* notes 10-12 and accompanying text.

172. *See generally* Hillberg, *supra* note 36 (discussing the extra data that will be created, and the various mediums that will arise as avenues to reach consumers in their vehicles).

173. *Id.*

174. *Id.*

175. *See, e.g.*, Kohler & Colbert-Taylor, *supra* note 34, at 121-23 (comparing intrusive in-car data collection and in-car targeted advertising to Steven Spielberg's film *Minority Report*).

176. Lin, *supra* note 2.

will be able to influence, and even control, the vehicle and its user.[177] The ways that marketers and businesses will be able to reach and influence drivers are far-reaching, with possibilities ranging from pop-up advertisements on the dashboard or windshield,[178] to potentially determining routes taken by the vehicle.[179]

In this hyperactive age of advertising, marketers will make certain that they take advantage of any opportunity to reach consumers, and will utilize any medium available to them to do so.[180] Therein lies the first potential issue with connected vehicle technology: in-car delivery of advertisements.[181] As discussed in the futuristic scenario advanced in Part I,[182] marketers will be able to utilize their full array of collected consumer information to target drivers with advertisements that are calculated towards attracting their attention and drawing their business.[183] These advertisements will be able to be delivered based upon where a car is traveling at any given time, thus allowing the vehicle to ask its driver whether she would like to stop in for a latte as she approaches a Starbucks location.[184] While these not-so-subtle nudges to drivers—reminding or urging them to take a detour and make a pit stop to purchase something of interest to them—might seem like a great convenience to some, it would most certainly be viewed as a nuisance or unnecessary intrusion by many.[185] Statistics regarding online advertising suggest that pop-ups, banners, and other types of simple online advertisements annoy an enormous number of consumers and Internet

177. *Id.*

178. *Id.*

179. Kohler & Colbert-Taylor, *supra* note 34, at 122-23.

180. *See* Shubham Jain, *Different Types of Modern Advertising Methods*, LINKEDIN (Apr. 2, 2015), https://www.linkedin.com/pulse/different-types-modern-advertising-methods-shubham-jain. Different methods of modern advertising include: print, guerrilla, broadcast, outdoor, public service, product placement, cellphone and mobile, and online (or digital) advertising. *Id.* In connected vehicles, marketers could utilize a combination of a number of these methods, including online, mobile, and broadcast advertising. *See id.*

181. *See, e.g.*, Hillberg, *supra* note 36; Lin, *supra* note 2. BMW has developed a program which would allow businesses to deliver in-car advertisements to drivers through the vehicle's navigation system. Tim Beissmann, *BMW Developing In-Car Advertising App*, CARADVICE (Jan. 24, 2014), http://www.caradvice.com.au/267639/bmw-developing-in-car-advertising-app. An example of the capabilities of this program would be to allow the navigation system, as the driver is traveling, to offer "large volumes of real-time offers generated by location based service providers." *Id.*

182. *See supra* Part I.

183. *See supra* Part I.

184. Lin, *supra* note 2; *see supra* Part I.

185. *See* Erika Morphy, *Online Ads Still Annoying Consumers*, CMSWIRE (July 26, 2016), http://www.cmswire.com/customer-experience/online-ads-still-annoying-consumers (discussing the nuisance created by advertisements on the Internet).

users.[186] As of July 2016, there were approximately 198 million active users of "adblock" software, a number that has surely grown since that time, and continues to grow today.[187] It would be perfectly logical to come to the conclusion that, if over 200 million consumers are displeased with advertisements showing up while they browse the Internet, a significant portion of drivers would find advertisements delivered to them in their connected vehicle to be just as much of an undesirable nuisance.[188] Beyond simply being an inconvenience, targeted advertising delivered in-car could pose an ethical issue.[189] Primarily, if these advertisements are delivered to cars that are not self-driving, the already prevalent danger of distracted driving could be made even worse.[190] With more content being delivered to dashboards, there will be even greater motivation for drivers to take their eyes off of the road, potentially causing a significant increase in accidents, injuries, and death, which again, would be the antithesis of the true purpose of connected vehicle technology.[191]

More troublesome than simply delivering advertisements, which could annoy or distract drivers, is the very realistic possibility that marketers and other third parties will be able to control the routes that connected cars drive when their user inputs a destination.[192] This possibility is not the least bit far-fetched—in fact, taxi drivers and hotel concierges have been known to accept payments from various businesses in exchange for steering business their way, or driving past their establishments.[193] This practice, as of now, seems to be lawful.[194] It would occur where there is no route to a user's desired destination that is clearly the "right" one, such as where multiple routes are similar in

186. *Id.*

187. *Id.* In addition to the adblock statistics, there was also a drop in user satisfaction with Facebook and Twitter in 2016, with drops of nine percent and eight percent respectively. *Id.* A portion of that dissatisfaction is likely a result of excessive advertising and a change in algorithm. *Id.*

188. *Id.* (discussing the general disapproval of online targeted advertising).

189. Lin, *supra* note 2.

190. *Id.* A study conducted in 2013 suggested that the problem of distracted driving had expanded as the usage of smartphones expanded, especially to older generations. Paresh Dave, *L.A. Auto Show: Distracted Driving Stalls App Integration into Cars*, L.A. TIMES (Nov. 20, 2013), http://articles.latimes.com/2013/nov/20/autos/la-fi-hy-auto-show-distracted-driving-20131120. Further, about 3300, or ten percent, of vehicle-related deaths in the two years leading up to the aforementioned study involved distracted driving. *Id.* Finally, in 2012, distracted driving caused over 400,000 injuries, according to the NHTSA. *Id.*

191. *See supra* Part II.A.

192. Kohler & Colbert-Taylor, *supra* note 34, at 122-23; Lin, *supra* note 2.

193. Lin, *supra* note 2.

194. *Id.*

terms of distance or travel time, or both.[195] In this scenario, the route planning could ostensibly be left to private commercial entities—those entities would pay to have the selected route be one that *just so happens* to take the vehicle past their establishment.[196] The fact that this would occur without the driver's knowledge would again raise ethical questions.[197] For example, there could be a situation where a person is attempting to diet, and is repeatedly routed past fast food restaurants because of her prior actions.[198] Ditto, a recovering alcoholic who is routinely routed past bars.[199] What if a driver has a restraining order against him, but his car is routed into an area he is legally forbidden from entering?[200] The lack of any user control in this situation is extremely troublesome—one scholar even went so far as to liken third-party control of the vehicle and its routes to a "mini-carjacking."[201] It is each of the aforementioned issues, dangers, and unanswered questions that create the drastic need for regulations regarding connected vehicle data collection, in-car advertising, and third-party control of those vehicles.[202]

IV. SOLVING THE RIDDLE: PROTECTING CONSUMERS AND A VITAL BUDDING TECHNOLOGY WITH SIMPLICITY, TRANSPARENCY, AND COMPLETE CONSUMER CONTROL

Connected and autonomous vehicle technologies were developed with very specific purposes in mind: safety and efficiency.[203] These technologies, at their core, are designed to serve the main purpose of

195. *Id.*

196. Kohler & Colbert-Taylor, *supra* note 34, at 122. Past driving and shopping habits, along with online activity, could be analyzed to determine the places where a driver might be most likely to stop and make impulse purchases. *Id.* Then, with that information, businesses and advertisers could pay to have that person routed by their store locations whenever possible. *Id.* Yet another example of this practice would be a gas station paying for drivers to be routed to its station when a car in the area needs to be refueled and uses its vehicle's GPS to find a station to go to. *Id.* at 122-23.

197. *Id.*; Lin, *supra* note 2.

198. Lin, *supra* note 2.

199. *Id.*

200. *See id.* (raising the question of who would be at fault if a connected, self-driving car drove a registered sex offender within the area surrounding a school that she is restricted from entering).

201. *Id.*

202. *See* Kohler & Colbert-Taylor, *supra* note 34, at 121 (noting the fact that federal privacy law, with respect to connected vehicle technologies, is "extremely underdeveloped").

203. Jeffrey Zients & John P. Holdren, *American Innovation in Autonomous and Connected Vehicles*, WHITE HOUSE (Dec. 7, 2015, 3:53 PM), https://obamawhitehouse.archives.gov/blog/2015/12/07/american-innovation-autonomous-and-connected-vehicles.

preventing human error, and thereby accidents, and reducing traffic in order to create a more efficient commuter system.[204] In order to fully utilize these technologies and realize their core purposes, which truly would revolutionize the roads, regulation must be enacted to make certain that other, unintended uses of the technology do not cause its downfall.[205] The issues discussed above—such as using these vehicles to collect data from drivers in order to combine that information with their "online profile" and target them with advertisements—have the power and potential to turn consumers off to connected vehicle technology, and destroy a very realistic hope for safer, improved roadways.[206]

In order to accomplish this, there are a number of steps that should be taken. First, the collection of personal information, and subsequent use of that information to target consumers with advertisements and offers tailored specifically for them, must be situated as an opt-in, rather than opt-out, service.[207] In addition to taking this step, the government must take initiative to ensure that, for those who do decide to opt-in to in-vehicle data collection and targeted advertising, there is complete transparency and safeguards to prevent abuse of consumer tracking.[208] This could be accomplished by promulgating specific guidelines to be followed by automakers and data brokers, similar to those that have been called for by numerous government agencies in regard to data collection over the Internet.[209]

A. Connected Vehicle Information Collection and Targeted Advertising Within the Vehicle Should Be an Opt-In, Rather Than Opt-Out, System

Current law, as it relates to data collection and processing over the Internet (via websites, social media, etcetera), provides very little protection for consumers.[210] As discussed earlier, a startling majority of consumers do not realize just how much information is being collected from them, nor how personal that data truly is.[211] While there is no statutory right for consumers to be able to opt-out of data collection, there are many services that provide them the ability to do so.[212] In

204. *Id.*
205. *See supra* Part III.
206. *See supra* Part III.
207. *See infra* Part IV.A.
208. *See infra* Part IV.B.
209. *See infra* Part IV.B.
210. *See* Hutchinson, *supra* note 22, at 1177-81 (discussing the vast unregulation of the data market and the few protections for consumers).
211. *See supra* note 35 and accompanying text.
212. *See, e.g.*, William J. Fenrich, Note, *Common Law Protection of Individuals' Rights in*

addition, many companies have privacy policies on their websites, which consumers wrongly believe provide them with security for their information,[213] and also allow consumers to opt-out from data collection on their site.[214] The issue, however, is that a large number of Americans are unaware of this ability.[215] Even if they do know about it, opt-out procedures are often cumbersome, time consuming, and inconvenient.[216] Therein lie the major issues with opt-out systems.[217] While they may seem to provide sufficient protection and choice for consumers, they are often merely a facade.[218] With an entire new system, source, and method of data collection cruising over the horizon, it is imperative to correct the flaws of simple online consumer protections and adopt an opt-in system for connected vehicle data collection.[219] As mentioned earlier, opt-in systems have already been put into place in regions with increased interest in protecting privacy rights of consumers, such as the EU.[220] If this step is taken, it would allow for a "best of both worlds" scenario, where those who are tech-entrenched and ultra-connected will be able to benefit from all of the perks and positives of targeted advertising, but those who would find it to be a nuisance or those who are very sensitive about protecting their data and maintaining a sense of privacy will easily be able to prevent themselves from being subject to these new services.[221]

If adopted, an opt-in system could take any one of a few different forms.[222] It might arise as an "all-or-nothing" situation, where consumers would decide to opt-in, or not, to data collection and targeted advertising in toto—that is, they would be allowing any company or any business

---

Personal Information, 65 FORDHAM L. REV. 951, 962-63 (1996).

213. Hutchinson, *supra* note 22, at 1168. Often, these privacy policies are very confusing to the average consumer. *Id.*

214. *See* Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1496 (2001).

215. *Id.* Not only do many Americans not know they can opt-out of data collection, but companies, on the whole, often make little effort to give notice of that ability. *Id.*

216. *See* Jeff Sovern, *Opting in, Opting out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1074-75 (1999).

217. Hatch, *supra* note 214, at 1495-98.

218. *See id.* (noting three fundamental flaws of opt-out systems: that they are conditioned upon individuals being able to understand how companies are using their data, that they are conditioned upon individuals getting meaningful notice of their right to opt-out, and that they are conditioned upon consumers being able to make the decision to opt-out without undue burden).

219. *See supra* notes 207-16 and accompanying text.

220. *See supra* Part II.C.2.

221. *See* Hatch, *supra* note 214, at 1494, 1498-99.

222. *See, e.g.*, *id.* at 1498-501 (discussing opt-in systems as a whole).

that utilizes the technology to track them.[223] The other scenario would be more complex, but likely be of greater interest and acceptance to consumers—there, they would be able to select specific businesses, perhaps from a list of all approved companies who utilize connected vehicle technologies, from which they are comfortable and willing to have their data collected and used to target them with advertisements.[224] In effect, this would be similar to subscribing to something on the Internet today.[225] In either case, consumers would reap the benefits of far greater protection.[226] Requiring a consumer's affirmative consent before collecting any information from her via her connected vehicle will ensure that her rights to privacy are not unknowingly infringed upon any more than they already have been.[227] Consumers will be provided with the option of "selection" as to how they desire to interact with and utilize this technology[228]—an opportunity to make a decision when presented with clear information about what data will be collected, how it will be used, and with whom it will be shared.[229] In addition to greater protections of privacy rights and an increased opportunity for consumer choice, an opt-in system would also provide for a more level playing field between consumers and businesses.[230] The current landscape of consumer tracking on the Internet has placed businesses in a position of extreme power.[231] Implementing an opt-in system would level that relationship a great deal, because it would allow for consumers to know exactly what information is being collected from their vehicle, and how that data would be used.[232] Finally, an opt-in approach would not only prove to be beneficial for consumers, but also for businesses.[233] If the latter of the two possible opt-in systems were implemented—where consumers would be able to opt-in on a company-by-company basis—businesses would reap the benefit of getting affirmative information

223. *See* Hutchinson, *supra* note 22, at 1181.

224. *See id.*

225. *See id.* For further discussion of the desire for maintenance and monitoring of companies engaged in the connected vehicle data market, see *infra* Part IV.B.

226. Hutchinson, *supra* note 22, at 1181-82.

227. *See* Hatch, *supra* note 214, at 1499-500 (discussing the parallel between an opt-in system and the reasonable expectation of consumers to keep their information private).

228. *Id.* at 1498-99.

229. *See infra* Part IV.B.

230. Hatch, *supra* note 214, at 1500.

231. *See supra* Part II.C. The fact that most consumers do not have any idea just how much advertisers know about them, and how personal that information is, is a clear indicator of the imbalance of power between consumers and the companies who "track" them. *See supra* Part II.C.

232. *See* Hatch, *supra* note 214, at 1500 (explaining this concept in the context of personal data collection in general).

233. *Id.* at 1500-01.

about which specific consumers are interested in their products or services.[234] This would allow for more efficient advertising and a decrease in wasted marketing expenses.[235] All told, implementing a successful opt-in program for connected vehicle data collection, dissemination, and use in targeted advertising, would create a safe and smart environment for this emerging, futuristic technology, and one that provides mutual benefits to all parties involved.[236]

B. The FCC Must Promulgate Guidelines to Ensure that Vendors Utilizing Tracking Technology Do Not Abuse It, and Inform Consumers of the Information Being Collected from Them

In order to properly safeguard consumers in connected vehicles, even with the adoption of an opt-in system, responsible agencies must promulgate strict guidelines for data-collecting companies, data brokers, and automakers to follow.[237] These guidelines should include rules and regulations regarding companies' duty to be transparent with consumers about what information they will collect, how it will be used, whether it will be shared, and with whom it will be shared.[238] Further, there must be a convenient, user-friendly method, for those who do opt-in to this technology, to be able to see what information is being collected from them, and to opt-out of these services via a simple action (whether they do so in toto or on a company-by-company basis).[239] Ideally, a centralized location or website where all of this could be accomplished would be created.[240] Finally, there should be a mandate for automakers to include the ability to view this information, and even to opt-out, from the infotainment systems they install in their vehicles.[241]

The idea of providing greater protections for consumers in the field of data collection is not foreign in America.[242] In fact, the U.S.

234. *Id.* at 1500.

235. *Id.*

236. *See supra* notes 208-33 and accompanying text.

237. *See, e.g.*, Hutchinson, *supra* note 22, at 1184-85 (providing suggestions for regulation of the data-broker industry).

238. *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACTION 49-53 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

239. *Id.* at 50-51.

240. *Id.*

241. *See id.* (mentioning the concept of locating all of this information in an easy to access, centralized location, which is the main objective underlying all variations of this idea, including doing so on a vehicle's infotainment system).

242. *See id.* at 49-54; U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 126, at 46; WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING

government and certain legislative agencies have made proposals to adopt rules, similar to those being proposed in this Note, to be enacted in order to protect individuals using the web and being "tracked" by cookies.[243] While there has not been much progress made on setting these recommendations into motion for online use,[244] it would be foolish to allow an entirely new realm of technology to come into existence without promulgating some regulations to control it, so as to avoid the massive issues that have arisen with simple Internet data collection.[245] In a report issued a few years ago, former President Barack Obama and the White House set forth a "Consumer Privacy Bill of Rights"—a set of proposed initiatives based upon providing and preserving consumers' rights, with regard to data collection, to "individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability."[246] There is a call to enable consumers to exercise complete control over what personal data is collected from them, and how it is used; to be provided with easily digestible and accessible information about their data; to have their data used only in the context for which it was provided; and to be given the ability to access, assess, and even correct that data which has been collected from them.[247] Finally, the report calls on the Federal Trade Commission ("FTC") to enforce these initiatives[248] and for Congress to codify them.[249] The United States Government Accountability Office ("GAO") has also issued a report on data collection.[250] In its report, specific attention is paid to information resellers, such as the data brokers discussed earlier.[251] In addition to an extensive discussion of its own findings, most of which align with the alarming privacy issues discussed above,[252] the GAO recommended that Congress "consider strengthening the current consumer privacy framework to reflect the effects of changes

---

PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 35-39 (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (each providing a different set of research, findings, and recommendations to better protect consumers who use the Internet).

243. *See* FED. TRADE COMM'N, *supra* note 238, at 49-54; U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 126, at 46; WHITE HOUSE, *supra* note 242, at 35-39.

244. *See supra* Part III.A.

245. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 126, at 46 (stating that the advent of advanced technologies has tremendously increased the amount of data being collected, and subsequently, the need for new legislation).

246. WHITE HOUSE, *supra* note 242, at 10.

247. *Id.* at 11-20.

248. *Id.* at 29-30.

249. *Id.* at 35.

250. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 126.

251. *Id.* at 1.

252. *See supra* Part III.

in technology and the marketplace—particularly in relation to consumer data used for marketing purposes."[253] Further, the report specifically mentions the possibility of making necessary changes in the permitted sources and methods of data collection and development of "privacy controls related to new technologies."[254] The FTC has also published a report regarding the issues arising from personal data collection and sharing, and has recommended taking steps very similar to those advanced by the White House and GAO.[255]

It is clear that in the years since these reports were issued, there has been essentially no progress made on enacting legislation to provide a general right of privacy to consumers in America.[256] With each passing year, creating overarching laws becomes more and more difficult, however, it is imperative that new technologies that are forthcoming, specifically connected vehicles, are outfitted with the proper legislation.[257] For that reason, Congress must work hand in hand with the FTC and other relevant agencies, to take the suggestions advanced in the reports discussed above, tailor them specifically to connected vehicles, and set them into action by enacting legislation to enforce them.[258]

First, all companies who wish to engage in collecting data from vehicles and/or using connected vehicles as a conduit for the delivery of advertisements should be required to register with a centralized agency or organization.[259] When they register, each company should clearly and simply state its policies, procedures, and intended actions with respect to the technology.[260] This registration process will serve multiple purposes: ensuring that there is more control over who can access connected vehicle data, ensuring compliance with the guidelines that will be enacted, forcing companies to create policy statements that are easy to understand for consumers, and gathering all companies who are participating in the technology in one central registry.[261]

---

253. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 126, at 46.

254. *Id.* at 47.

255. *See* FED. TRADE COMM'N, *supra* note 238, at 49-54.

256. *See supra* Part III.

257. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 126, at 46-47 (stating the importance of developing privacy controls for emerging technologies).

258. *See* FED. TRADE COMM'N, *supra* note 238, at 49-54; U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 126, at 46-47; WHITE HOUSE, *supra* note 242, at 11-22, 29-30.

259. *See* FED. TRADE COMM'N, *supra* note 238, at 6 (discussing a similar proposal set forth by the FCC, intended to regulate data brokers).

260. WHITE HOUSE, *supra* note 242, at 14-15.

261. *See id.* (discussing the benefits of a "transparent" disclosure requirement, such as the one discussed above).

Next, the list of companies and their intended uses of connected vehicle data should be curated into a single, easily navigable list, located on one platform.[262] This would be best suited for a single website.[263] Further, on that centralized website, consumers should be able to log in to an account they create, where they would be able to view a list of the companies that they have opted into, see what information has been collected about them, and easily be able to opt-out from any one, or all, of those companies' targeted advertising services.[264] Finally, automakers should be required, when programming the infotainment systems to be placed in their connected vehicles, to provide an easy way for drivers to access the database described above, and to utilize it the same way they would on the web.[265]

V. CONCLUSION

Connected and autonomous vehicles are approaching reality at an incredible pace, and it will not be long before these futuristic machines become commonplace on the roads of America.[266] This incredible leap in technological capabilities should provide invaluable increases in safety and efficiency on the road, and a sharp decrease in vehicle accidents and deaths that occur because of human error.[267] However, there is a threat to the advancement and persistence of this technology.[268] The invasion of consumer privacy, collection and distribution of personal information, and persistent targeted advertising that annoys and concerns hundreds of millions of people could soon be taken to an entirely new level in connected vehicles.[269] The constant stream of data flowing into and out of connected vehicles, along with the newly available, highly sought after geographic data points, would allow marketers and data brokers to obtain unprecedented access into consumers' every move.[270]

---

262. *See* FED. TRADE COMM'N, *supra* note 238, at 6.

263. *See id.*

264. *See id.* at 50-51 (proposing a similar centralized database to be used specifically for data brokers).

265. *See* WHITE HOUSE, *supra* note 242, at 14-15 (advocating the right of consumers to have access to "easily understandable and accessible information"); *see also supra* note 239 and accompanying text.

266. *See supra* Part II.A–B.

267. *See, e.g.*, Zients & Holdren, *supra* note 203.

268. *See supra* Part III.

269. *See supra* Part III.

270. *See supra* notes 171-73 and accompanying text.

In order to prevent connected vehicle technology from becoming yet another unwanted technology, and to ensure that it is able to help create safer, smarter, and more efficient roadways, Congress must pass necessary legislation.[271] Making data collection and targeted advertising in connected vehicles an opt-in service, rather than opt-out, will allow all users of connected vehicles to easily make a choice regarding the pros and cons of those services.[272] Those who want advertisements and offers from certain companies will be able to receive them, but those who do not will easily be able to avoid them while still enjoying the safety and efficiency for which these systems are designed.[273] Further, rules and regulations must be enacted in order to properly utilize the opt-in system.[274] These rules should require registration of companies, along with clear and concise statements of intended use, which can be placed onto a centralized portal.[275] From that portal, drivers should be able to read companies' statements, see what data has been collected from them, and most importantly, opt-in and -out.[276] Finally, automakers should be forced to install the ability to interact with this portal from infotainment systems in connected vehicles.[277] If each of these steps is taken, it will ensure that consumers are given the most fair and convenient way to utilize this incredible technology, and allow for every user to enjoy her own ideal service.[278]

*Brandon Amon**

271. *See supra* Part IV.
272. *See supra* Part IV.A.
273. *See supra* Part IV.A.
274. *See supra* Part IV.B.
275. *See supra* Part IV.B.
276. *See supra* Part IV.B.
277. *See supra* Part IV.B.
278. *See supra* Part IV.

* J.D. Candidate 2018, Maurice A. Deane School of Law at Hofstra University. I would first like to thank my parents, Lori and Mark, for everything you have done for me. You have been a constant source of strength, encouragement, and love, and for that I owe you everything. To Sara DiCandia, for not only putting up with me throughout three stressful years of law school, but for all of your love, and for being my rock in all facets of my life. To all of my family and friends, of which there are far too many to thank individually, for being by my side no matter what. I am extremely lucky to have you all. A special thank you to the Volume 46 Managing Board—Jonathan DeMars, Tessa Patti, and Mindy Hollander—as well as Savannah Holzwarth, and Alexis Fallon whose hard work and dedication has ensured the continued success of the *Hofstra Law Review*, and without whom the publication of this Note surely would not have been possible. Finally, a very special thank you to my grandfather, Robert Katz. You were the greatest teacher, role model, and positive influence in my life. I owe my passion for the field of law to you, and I will continue to strive each and every day to make you proud. I love you and miss you dearly.