The Roads of the Future Require a Functioning P.A.V.E.R.: How Autonomous Vehicles are More Like Your Bank Than Your Browser, and Must be Regulated Accordingly

Brian R. DeMocker*

TABLE OF CONTENTS

* J.D., May 2020, The George Washington University Law School. Thank you to my loving parents, sister, and brother-in-law for offering wisdom, support, and patience throughout my education. Thank you to my wonderful fiancée for insightfully advising me and protecting my sanity throughout both this writing process and all of law school. I could not have reached my goals without each of you. Thank you to the staff of the Federal Communications Law Journal for their patience, hard work, and assistance with this publication.

I. INTRODUCTION

It is Friday evening and you just clicked "send" on your computer, which completes a *long* week at your law firm. As your completed memorandum navigates cyberspace, your phone blinks awake to receive your verbal instruction to hail a self-driving, "autonomous" vehicle to meet you at the curb. A vehicle pulls up as you exit your building and you climb in through the opened doors. As you stretch your legs out in front of you, the screen illuminates to display a list of destination options. Brewery, brewery, cocktail bar, brewery, brewery, home. They know me too well, you muse. It is 6:45 PM and you have, after all, gone to a brewery every Friday after work. You select one of the breweries and the vehicle silently speeds toward the destination.

On your way, you check the news to find a new piece of federal legislation up for consideration called the Privacy in Autonomous Vehicles and Enforcement Regulation, or "P.A.V.E.R.," which would allow connected and autonomous vehicle users to opt out of the commercial exploitation of nonpublic personal information, such as vehicle location data, collected by connected or autonomous vehicles[1] in order to limit the information that can be used in targeted advertisements. After reading further about P.A.V.E.R., you recall that on Monday you must drive to the headquarters of a largely controversial political group in order to deliver some files related to an ongoing dispute between one of your clients and the group. You realize that if you use an autonomous vehicle, or even a connected vehicle that is not fully autonomous, your route and destination would be recorded and attached to your online marketing profile, which would cause you to begin receiving targeted advertisements relating to the controversial group. You realize that P.A.V.E.R. would actually allow you to decide that this particular errand would go unrecorded. Suddenly, P.A.V.E.R. earns you as a new fan.

Seeing as P.A.V.E.R. is not yet implemented, you weigh alternative options for keeping your errand unrecorded. You ultimately elect to rent (at your firm's expense, of course) a cheap, non-connected, and non-autonomous vehicle for the errand to avoid digital association with the controversial group, despite the fact that you have not actually driven a vehicle manually in many years.

Monday arrives and you climb into the old, non-autonomous vehicle with your files in tow. You feel a little cramped due to the presence of a steering wheel. How antiquated, you think. You put the vehicle into reverse manually and press down on the gas pedal, which makes the vehicle lurch backwards abruptly. After you gather yourself, you ease the vehicle backwards and take off down the road. After about thirty minutes of jerky driving, you glance at the right side-mirror to find a bicyclist only inches from

1. "Connected" vehicles shall refer to vehicles that have the ability to receive, process, and transmit data to other connected vehicles, infrastructure, and/or the Internet. "Autonomous" or "partially-autonomous" vehicles shall refer to vehicles with the ability to "self-drive," or operate with no or minimal driver intervention.

your vehicle. Startled and unused to manually operating a vehicle so close to another person, you jerk the wheel left, causing the non-autonomous vehicle to jump the curb and slam into a concrete barrier. After a short stay in the hospital, you are discharged. P.A.V.E.R. would have avoided this whole situation.

Just as banks and financial institutions cannot disclose certain information about customer choices and buying habits to certain unaffiliated third-party entities due to restrictions on sharing nonpublic personal information following customer opt-out,[2] autonomous vehicle manufacturers should not be permitted to disclose the data collected through regular vehicle operations (such as the vehicle's current location, home or work addresses, browsing histories on the vehicle's interfaces, or driving routes and times) to unaffiliated third-party entities unless the customer declines to opt out or unless such data sharing is necessary to properly operate the vehicle. Autonomous vehicles are much safer than conventional vehicles[3] and as such, mainstream use should be heavily incentivized. There exists, however, a data privacy concern stemming from the use of the information necessarily collected through regular autonomous vehicle (or any sort of connected vehicle) operation that could present a major barrier to mainstream autonomous vehicle use.[4] Unfortunately, there is a complete lack of federal restrictions on manufacturers' use of this information.[5] Thus, Congress should pass regulatory legislation directed at the autonomous vehicle industry in order to reduce the chilling effect that surveillance capitalism can have on individuals' freedom of expression and consumer choices, which would deconstruct barriers to the use of a vital transportation service capable of substantially reducing the number of vehicle-related injuries and deaths.[6] This paper will show how the Gramm-Leach-Bliley Act,[7] the banking and

2. 15 U.S.C. § 6802 (2012).

3. *See* Brandon Amon, *Invading the Driver's Seat: Preventing Overbearing Targeted Advertising in Connected Vehicles*, 46 HOFSTRA L. REV. 329, 353-54 (2017) (citing 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).

4. *See, e.g.*, United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").

5. Angela Stringfellow, *The Ultimate Data Privacy Guide for Banks and Financial Institutions*, NGDATA (Aug. 14, 2018), https://www.ngdata.com/data-privacy-guide-for-banks-and-financial-institutions/ [https://perma.cc/8DGL-VKWY] ("There's currently no overarching federal law addressing data privacy in full.").

6. *See generally Maximizing the Benefits of Self-Driving Vehicles: Principles for Public Policy*, UNION OF CONCERNED SCIENTISTS (Feb. 3, 2017), https://www.ucsusa.org/sites/default/files/attach/2017/02/Maximizing-Benefits-Self-Driving-Vehicles.pdf [https://perma.cc/TP5P-V5NM] [hereinafter UNION OF CONCERNED SCIENTISTS]; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., AUTOMATED DRIVING SYSTEMS 2.0: A VISION FOR SAFETY i (Sept. 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf [https://perma.cc/822T-MDKD] [hereinafter NAT'L HIGHWAY TRAFFIC SAFETY ADMIN.].

7. 15 U.S.C. § 6801–6809 (2012).

financial industry's data privacy regulation, provides a particularly adaptable regime well-suited for use by the autonomous vehicle industry.

Section II of this paper addresses the factual and legal background of both the autonomous vehicle industry and the banking and financial industry. Section III discusses three issues. First, it argues that the banking and financial industry is subject to certain regulations regarding use of nonpublic personal information unlike other data-driven industries, such as those offering web browsing or online shopping, because the products and services offered by banks and financial institutions are considered "vital" in today's society. It also discusses how autonomous vehicles are likewise distinguishable from data-driven companies and how such vehicles are more similar to banks and financial institutions. Further, Section III discusses how the Gramm-Leach-Bliley Act provides a useable template for regulation of the autonomous vehicle industry. Section IV proposes P.A.V.E.R. as a solution to the unregulated use of nonpublic personal information by autonomous vehicle manufacturers, describes P.A.V.E.R.'s construction, and discusses other solutions proposed in relevant scholarly literature. Finally, Section V addresses questions that must still be answered before society can make a fully informed decision about how to address data privacy in the autonomous vehicle industry, and finishes with a charge to Congress to pass legislation to effectively regulate data privacy in the autonomous vehicle industry. The primary focus of this paper is on private companies' use of nonpublic personal information and does not discuss governmental surveillance applications, which have largely been found unconstitutional.[8]

II. THE FACTS AND LAWS SURROUNDING THE AUTONOMOUS VEHICLE INDUSTRY AND THE BANKING AND FINANCIAL INDUSTRY

Discussion of both the autonomous vehicle industry and the banking industry is necessary to understand the comparison made later in this paper between the two industries. The autonomous vehicle section lays the foundation for the argument that the industry is "vital" due to the ability of autonomous and connected vehicles to reduce traffic fatalities and injuries,[9] and that the use of such vehicles will become well integrated into society.[10] The banking and financial section lays the foundation for the argument that the industry is "vital" due to the deep societal integration of the use of, and financial protection by, the products and services offered by banks and financial institutions. [11] These sections also provide the background information needed to understand the later argument that the financial

8. *See, e.g.*, *Jones*, 565 U.S. at 400-13 (holding that the warrantless collection of location data through attachment of a GPS device violated the Fourth Amendment).

9. *See generally* UNION OF CONCERNED SCIENTISTS, *supra* note 6; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 6, at i.

10. *See infra* Section II.A.

11. *See infra* Section II.B.

industry is regulated largely due to its "vital" nature and, as such, the autonomous vehicle industry should be similarly regulated.[12]

A. The Autonomous Vehicle Industry

To best grasp the workings of the connected and autonomous vehicle industry and the vehicles themselves, inquiry into the factual and legal background is an important first step. Autonomous vehicles operate at different levels of automation, which influences the type and amount of information necessarily collected for the vehicle to function properly.[13] As vehicles become more advanced and require less human intervention, the collection and use of a larger amount of data is required.[14] There is not currently, however, any federal legislation that limits how this data can be used, despite its high risk of abuse.[15]

1. How Autonomous Vehicles Function and Inherent Privacy Threats

Automotive companies are beginning to entertain the idea that autonomous vehicles are the next step in innovation and road safety.[16] In fact, some experts say that autonomous vehicles may be the most important transportation innovation since the inception of the automobile.[17] Autonomous vehicles are those designed to transport people and cargo to a destination, requiring varying levels of reduced human intervention and focus, ranging from heavily human-controlled to fully self-driving.[18] Researchers have labeled the different levels of vehicle automation as follows: Level 0 refers to full human control; Level 1 refers to when the vehicle controls certain systems, such as braking or cruise control; Level 2 refers to when the vehicle operates using multiple automated functions, such

12. *See infra* Section III.

13. *See infra* Section II.A.1.

14. *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, 103-04 (2015); *see also Self-Driving Cars Explained*, UNION OF CONCERNED SCIENTISTS (Jan. 26, 2017), https://www.ucsusa.org/clean-vehicles/how-self-driving-cars-work#.XDoTTM9KjzJ [https://perma.cc/7AYJ-DURS]; *infra* Section II.A.1.

15. *See infra* Section II.A.2.

16. *See generally Looking Further: Ford Will Have a Fully Autonomous Vehicle in Operation by 2021*, FORD, https://corporate.ford.com/articles/propulsion-choices/autonomous-2021.html [https://perma.cc/BJD8-46XY] (last visited Oct. 9, 2019); *see, e.g.*, Andrew Giambrone, *Ford to Test Driverless Cars in D.C. Early Next Year*, CURBED (Oct. 22, 2018, 5:32 PM), https://dc.curbed.com/2018/10/22/18010858/dc-ford-driverless-cars-autonomous-vehicles-transportation [https://perma.cc/6GNF-UGGM] (last visited Oct. 9, 2019); *Future of Driving*, TESLA, https://www.tesla.com/autopilot [https://perma.cc/5WQH-2GY9] (last visited Oct. 9, 2019); WAYMO, https://waymo.com/tech/ [https://perma.cc/F67F-R97Z] (last visited Oct. 9, 2019).

17. *See* UNION OF CONCERNED SCIENTISTS, *supra* note 6.

18. *See* Kohler & Colbert-Taylor, *supra* note 14, at 102-03; *see also* UNION OF CONCERNED SCIENTISTS, *Self-Driving Cars Explained*, *supra* note 14.

as steering plus acceleration and braking, but humans must remain focused and alert in the event that intervention is necessary; Level 3 refers to when the vehicle can operate safely by itself in nearly all situations and under certain conditions; Level 4 refers to when the vehicle can operate safely and autonomously in nearly all situations and under any condition; and, although some researchers end after Level 4, Level 5 refers to when the vehicle is entirely capable of self-driving in any situation and in any condition.[19]

To create a functioning autonomous vehicle that can operate at Levels 2 through 5 (and sometimes even for Level 1), vehicle manufacturers must install on-board sensor-based solutions, vehicle-to-vehicle ("V2V") and vehicle-to-infrastructure ("V2I") connectivity-based solutions, or more likely a combination of both solutions, to enable the vehicle to avoid hazards in and around the roadway.[20] On-board computers can evaluate environmental and vehicular data received from on-board sensors, such as speed, acceleration, vehicle roll angle, heading, information about the surroundings, current location, and more, which is essential to the safe operation of the vehicle.[21] Connectivity-based solutions allow vehicles to determine the speed and direction of other vehicles sharing the road, and routing information about the other vehicles' destinations.[22]

While Level 1, 2, and 3 autonomous vehicles have already rolled out and are in use or in testing today,[23] fully autonomous (i.e., entirely self-driving) vehicles are still to come.[24] There are, however, data privacy concerns relevant to the Level 1, 2, and 3 V2V-capable vehicles that have already been released.[25] Juniper Research released a study in December 2018 projecting that "over 62 million vehicles will be capable of V2V . . . communication by 2023" and that by then, 60% of all new sales of vehicles in the US will have V2V capability.[26] The research also noted that long "vehicle refresh rates" (meaning the time it takes for an owner to sell or dispose of a vehicle and buy a new one), which are generally around eight to twelve years, will "hinder mass adoption" of V2V technology in the immediate future.[27] This means that there are vehicles that are already, or soon to be, on the road that have the capacity to share certain data gathered

19. *See* Kohler & Colbert-Taylor, *supra* note 14, at 102-03; *see also* UNION OF CONCERNED SCIENTISTS, *Self-Driving Cars Explained*, *supra* note 14.

20. *See* Kohler & Colbert-Taylor, *supra* note 14, at 103-04.

21. *See* Michael Mattioli, *Autonomy in the Age of Autonomous Vehicles*, 24 B.U. J. SCI. & TECH. L. 277, 283-84 (2018).

22. *See* Kohler & Colbert-Taylor, *supra* note 14, at 126-27.

23. *See, e.g.*, *Future of Driving*, TESLA, https://www.tesla.com/autopilot [https://perma.cc/R5TM-59EY] (last visited Oct. 13, 2019).

24. *See* Kohler & Colbert-Taylor, *supra* note 14, at 103.

25. *See, e.g.*, Amon, *supra* note 3, at 350-52.

26. *See Vehicle to Vehicle Communications To Be Installed in 62M Vehicles by 2023, As 56 Disrupts Established Automotive Strategies*, JUNIPER RESEARCH (Dec. 11, 2018), https://www.juniperresearch.com/press/press-releases/vehicle-to-vehicle-communication-to-be-installed [https://perma.cc/8V5B-XE83].

27. *See id.*

by the vehicle despite not requiring this V2V connectivity in order to function properly as a viable transportation option.[28]

The data gathered by an autonomous or connected vehicle would certainly aid in the vehicle's operation,[29] but the threat of data misuse may deter some individuals from using such vehicles. William J. Kohler and Alex Colbert-Taylor identified, in a 2015 article in the Santa Clara High Tech Law Journal, two major privacy concerns implicated if a private entity enjoyed unregulated control of the data generated by necessary operations of an autonomous vehicle: potentially invasive tailored advertising and private commercially-motivated route planning.[30]

The first concern, regarding advertisements, arises from what private entities can do with the data gathered from the vehicle to advance marketing interests.[31] Automobile manufacturers and other private companies have already obtained patents that address advertising inside private vehicles,[32] which indicates an interest in such advertising practices. Much like data brokers that gather information based on an individual's Internet usage to build an online advertising profile and push tailored advertising to that individual, vehicle manufacturers or other entities could achieve a similar outcome through analysis of a connected vehicle's travel habits.[33] These kinds of targeted advertisements are already in use throughout the Internet,[34] and as such it is not unreasonable to expect the practice to enter the autonomous vehicle industry. After all, in a Level 3 or above vehicle, where an individual does not need to intervene much, if at all, advertisers would enjoy a captive audience, as the vehicle's occupant or occupants would be able to browse the Internet rather than focus on the road.[35]

As previously stated, there may be nothing inherently wrong with receiving relevant, tailored advertisements. The mere possibility, however, that a third party may receive or purchase one's nonpublic personal information for targeted commercial exploitation can, according to Justice Sotomayor, have a chilling effect on individual expression.[36] While Justice Sotomayor focused her discussion in *United States v. Jones* on governmental monitoring and its effects on an individual's behavior,[37] it would be a logical leap and perhaps not that difficult to expand the scope to include non-governmental entities and the chilling effect that marketing-focused surveillance and data collection would have on an individual's behavior. Justice Sotomayor further discussed how location data could reveal details

28. *See id.*; *see generally* Kohler & Colbert-Taylor, *supra* note 14, at 120.
29. *See* Amon, *supra* note 3, at 342.
30. *See* Kohler & Colbert-Taylor, *supra* note 14, at 121-23.
31. *See id.* at 122-23.
32. *See id.* at 121-22.
33. *See id.* at 122.
34. *See id.*
35. *See, e.g.*, *id.*
36. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").
37. *See generally id.* at 413-18 (Sotomayor, J., concurring).

about an individual's family, political affiliations, professional life, religious beliefs, and sexual relations.[38] Some data privacy experts also "warn that this [type of data collection and distribution for marketing purposes] would open the door to harmful new forms of commercial surveillance."[39]

The second concern, regarding private, commercially-motivated route planning versus algorithmic routing, presents a troubling set of possibilities. Consider the ideal scenario for autonomous route planning: the vehicle, unprompted, is able to gather information from vehicle networks and Internet sources regarding weather and road conditions, pedestrian and non-autonomous vehicular congestion, and even hot-spots where anti-autonomous vehicle vandalism or violence is known to occur, and the vehicle is then able to plan a route accordingly. Consider the alternative, where a private entity controls route-planning functions: the vehicle performs the above algorithmic route planning, then incorporates the private entity's commercial interests. For example, the vehicle might route, and perhaps even select a longer route, to travel past the physical buildings of paying businesses.[40] Utilizing the individual's online advertising profile discussed above, the vehicle could select a route past businesses at which the vehicle's occupant would be most likely to stop and make a purchase.[41] Briefly exiting the realm of purely economic and commercial motivations, one can imagine another scenario where the route-controlling entity has political ties to other entities and could encourage vehicles to plan routes that travel in close proximity to the entities' political events.

2. The Laws Surrounding Autonomous Vehicles—or Lack Thereof

Although several states maintain their own data privacy regulations,[42] there is no single federal privacy law applicable to every jurisdiction in the United States that restricts the distribution or sale of data collected from an autonomous vehicle.[43] Congress has briefly entertained federal data privacy legislation applicable to autonomous or connected vehicles, but the proposed legislation would have provided little meaningful regulation and, in any case, has failed.[44]

Additionally, the Electronic Communications Privacy Act (ECPA), codified under 18 U.S.C. §§ 2510-2522 (2012), applies only to the

---

38. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *see also* Kohler & Colbert-Taylor, *supra* note 14, at 124.

39. *See* Mattioli, *supra* note 21, at 280.

40. *See* Kohler & Colbert-Taylor, *supra* note 14, at 122.

41. *See id.*

42. *See, e.g.*, Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N PRIVACY PROFESSIONALS (Apr. 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/ [https://perma.cc/9ZP8-XEG8].

43. *See* Stringfellow, *supra* note 5.

44. *See, e.g.*, H.R. 3388, 115th Cong. § 12(a) (2017) (failed); *see also* S. 680, 115th Cong. (2017) (failed).

interception of electronic communications.[45] The ECPA does not regulate what entities can do with information obtained through legal means, such as from the normal operation of an autonomous vehicle.[46] Furthermore, the Federal Trade Commission Act, codified under 15 U.S.C. §§ 41-58, applies to topics such as unfair or deceptive practices,[47] but similarly does not address what an entity may do with the sort of data collected from an autonomous vehicle.

Thus, there is currently no substantive federal law that could be applied to autonomous vehicle data privacy.[48] If autonomous vehicle manufacturers wanted to use or distribute nonpublic personal information collected from normal vehicle operations, the fact that autonomous vehicles are innately transportable across state lines would potentially force manufacturers to program vehicles to change their data sharing algorithms based on their current location.[49] And if a state passed new legislation amending its existing privacy legislation, manufacturers would need to quickly and remotely revise the vehicles' protocols for that jurisdiction in order to maintain compliance.

B. The Banking and Financial Industry

The banking and financial industry is a widely used source of products and services that is analogous to the autonomous vehicle industry in several ways discussed in future sections.[50] Consumers today frequently use banks and financial institutions, and the benefits are well established.[51] Through regular operations, these institutions also handle a large amount of nonpublic personal information, which can be abused.[52] As such, Congress passed federal legislation aimed at protecting consumers' data privacy.[53]

1. The Uses of, and Abuses by, Banks and Financial Institutions

Banks and financial institutions are widely used and heavily integrated into society.[54] According to a 2017 Federal Deposit Insurance Corporation (FDIC) survey, executed in partnership with the United States Census Bureau,

45. *See* 18 U.S.C. §§ 2510-2522 (2012).
46. *See, e.g.*, *id.*
47. *See* 15 U.S.C. §§ 41-58 (2012).
48. *See, e.g.*, Stringfellow, *supra* note 5.
49. This scenario could occur if state privacy legislation required that all vehicles (or any device capable of sharing data, for that matter) operating within its jurisdiction comply with the state privacy law.
50. *See infra* Section III.
51. *See infra* Section II.B.1.
52. *See infra* Section II.B.1.
53. *See infra* Section II.B.2.
54. *See generally* FED. DEPOSIT INS. CORP., FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS 1-14 (2018), https://www.fdic.gov/householdsurvey/2017/2017execsumm.pdf [https://perma.cc/JKX5-5DU4] [hereinafter *FDIC Survey*].

approximately 6.5% of households in the United States were "unbanked" in 2017, meaning that none of the individual members of the household possessed a bank account (either a checking or savings account).[55] Importantly, the survey also found that 68.4% of households were "fully banked," meaning the members of the household maintained bank accounts with insured institutions and did not use alternative financial services during the preceding 12 months.[56] The survey also revealed a trending decline in the rate of unbanked households from 2015 to 2017.[57] As more people and households turn to checking and savings accounts for everyday transactional convenience, privacy concerns grow.[58]

Banks and financial institutions regularly collect information and data from their customers in order to deliver financial products and services.[59] If a customer uses a credit card, or even just opens an account, the institution collects information such as name, address, contact information, income, wealth data, spending habits, and the location of purchases.[60] Moreover, financial transaction information can paint a detailed picture of an individual's private life without the individual realizing just how much detail can be discerned through analysis of that data.[61] Some examples of the sort of information that can be determined through transaction history include home or work addresses, home ownership status, rental relationships, age, medical information, prescribed medication, physical body details such as height and weight, income and debt levels, product preferences, political or religious affiliations, ethnic identity, marital status, family member details, travel and vacation habits, hobbies, and criminal tendencies.[62]

Some individuals may not care if banks and financial institutions sell the individual's depersonalized online profile to marketers or data brokers. Some may even welcome targeted advertisements informed by such transactional data because the advertisements would be more relevant to the individual. Others, however, may not appreciate targeted advertisements informed by the types of transactions in which the individual engages. It is not difficult to imagine the embarrassment that could stem from a situation where an individual is browsing his or her computer in public when, surprisingly, the individual's computer is flooded with targeted advertisements for products and services that reveal the individual's secrets. Imagine a teenage daughter's parents walking past her computer and seeing advertisements for baby formula, prenatal vitamins, maternity clothes, and strollers. Imagine an individual showing his friends or family an online video,

---

55. *Id.* at 1.
56. *Id.*
57. *Id.*
58. *See* Janet Dean Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 946-947 (2002).
59. *See* FED. DEPOSIT INS. CORP., YOUR RIGHTS TO FINANCIAL PRIVACY, https://www.fdic.gov/consumers/privacy/yourrights [https://perma.cc/4HSV-WV2X] (last visited Sept. 20, 2019) [hereinafter *FDIC Privacy Rights*].
60. *Id.*
61. *See* Gertz, *supra* note 58, at 944-48.
62. *See id.* at 944-45.

preceded by advertisements for Viagra or genital anti-fungus medication. Imagine still an abuser becoming enraged and violent after using his victim's computer and seeing advertisements for self-defense classes, self-defense weapons, or travel websites. The above possibilities are only a few scenarios with potentially disastrous outcomes. The point stands: a relatively small amount of nonpublic personal information, such as the information derived from financial transactions, can reveal a substantial amount more about an individual's life than that individual may be comfortable sharing.

2. Legislated Data Privacy, Courtesy of the Gramm-Leach-Bliley Act

Various laws recognize the privacy concerns articulated above and the need to protect certain customer behavior.[63] Congress passed the Federal Financial Modernization Act, also referred to as the Gramm-Leach-Bliley Act,[64] 15 U.S.C. §§ 6801–6809, to regulate and enhance fair competition in the banking and financial services industry.[65] Importantly, the Act also regulates how banks and financial institutions handle individuals' nonpublic, personal information by instituting a Congressional policy under Title V of the Act, requiring financial institutions to adopt "an affirmative and continuous obligation to respect the privacy of its customers."[66] As defined by the Act, nonpublic personal information refers to personally identifiable financial information that is not publicly available and is either provided to the bank or financial institution by the customer, received by the bank or financial institution through the customer's financial transactions or use of a service provided by the institution, or somehow otherwise received by the financial institution.[67] Furthermore, the Gramm-Leach-Bliley Act states that banks and financial institutions are prohibited from disclosing this nonpublic personal information to an unaffiliated third party, unless three conditions are satisfied.[68] First, the institution must "clearly and conspicuously" notify the customer that the institution may disclose the information to the third party; second, the customer must have ample opportunity prior to the disclosure to prohibit the institution from disclosing that information; and third, the institution must inform the customer how to exercise the opt-out option.[69]

There are, however, several critical shortcomings and loopholes in the Gramm-Leach-Bliley Act. First, there is debate as to the effectiveness an opt-out option would have on an individual's privacy.[70] The result of an individual opting out is not necessarily the individual's intended outcome. Once an

63. *See, e.g.*, 15 U.S.C. §§ 6801–6809 (2012).
64. *Id.*
65. *See* Gertz, *supra* note 58, at 982.
66. 15 U.S.C. § 6801(a) (2012).
67. *See id.* § 6809(4).
68. *See id.* § 6802(b).
69. *Id.*
70. *See* Andrew J. McClurg, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U.L. REV. 63, 133-34 (2003).

individual opts out of the data-gathering regime, compliance with the Gramm-Leach-Bliley Act requires only that banks and financial institutions refrain from sharing certain types of information with certain unaffiliated third parties, not that the banks and financial institutions cease data collection.[71] Additionally, the Act only applies to "financial institutions," such as banks and other like-institutions that are engaged in activities that are financial in nature (for example, lending, exchanging, transferring, investing for others, or safeguarding money or securities, and much more).[72] Therefore, entities that are not primarily engaged in activity that is financial in nature, such as large data companies, need not comply with the Gramm-Leach-Bliley Act and may freely disseminate nonpublic personal information to third parties.[73]

Furthermore, the Act does not prohibit a bank or financial institution from sharing nonpublic personal information with affiliated partners, including marketing partners that are not "third party," even over a customer opt-out.[74] This means that the Act does not specifically outlaw all sharing of individuals' nonpublic personal information if the customer opts out.[75] Thus, not all nonpublic personal information can be sheltered.[76] Large data companies certainly manage and use nonpublic personal information and share or sell that data to marketers and data brokers for use with targeted advertisements.[77] Yet, despite the aforementioned shortcomings, the banking and financial industry, and specifically the Gramm-Leach-Bliley Act, provides a useful template for how to regulate the autonomous vehicle industry.

III. HOW AUTONOMOUS VEHICLES ARE MORE LIKE THE BANKING AND FINANCIAL INDUSTRY AND WHY SUCH VEHICLES NEED DATA PRIVACY LEGISLATION

As previously discussed, autonomous vehicles will receive, process, and transmit a large amount of information through normal functions and

71. *See id.*

72. *See* 15 U.S.C. § 6809(3) (2012); *see also* 12 U.S.C. § 1843(k)(4) (2012).

73. *See* 15 U.S.C. § 6809 (2012); *see also Making It Easy to Understand What Data We Collect and Why*, GOOGLE, https://safety.google/privacy/data [https://perma.cc/4P7T-3JHN] (last visited Oct. 9, 2019); *Amazon Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html? nodeId=201909010 [https://perma.cc/7RWJ-PVVL] (last visited Oct. 9, 2019); *Data Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy [https://perma.cc/T9GT-NTKY] (last visited Oct. 9, 2019); *How Does Facebook Show Ads on Mobile Devices and Connected TVs?*, FACEBOOK, https://www.facebook.com/help/119468292028768?ref=dp [https://perma.cc/2MKJ-8NJK] (last visited Oct. 9, 2019).

74. *See* 15 U.S.C. §§ 6802 (2012).

75. *See id.*

76. *See, e.g.*, *Ads and data*, GOOGLE SAFETY CENTER, https://safety.google/privacy/ads-and-data/ [https://perma.cc/T77D-W6HP] (last visited Oct. 11, 2019); *see also* AMAZON, *supra* note 73; *Data Policy*, FACEBOOK, *supra* note 73.

77. *See id.*

operations.[78] Autonomous vehicle users will likely be very interested in whether this data can be used to add to, or update, their online marketing profiles.[79] Additionally, those users will want to know information such as "what uses are made of such personal data, why it is being collected, how it will be used, how long it will be kept, and who will and will not have access to it[,]" as well as whether the collected data will reveal "where, when, and how a person moves from geographical place to place[.]"[80] The consequences of allowing unfettered data collection vary widely. One concern on a smaller, individual scale is that the data collected will, in aggregate, reveal additional nonpublic personal information, which can be used to push unwanted, or even invasive, targeted advertisement campaigns to individuals.[81] This data could also be used to manipulate an individual's habits, such as travel destinations or what restaurants to visit.[82] Another concern on a larger scale is that the information from autonomous vehicles could be analyzed to reveal an enormous amount of information on particular large populations of individuals, or even all users, which allows those in control of the information to enjoy significant influence over those populations.[83]

To address privacy concerns that could stunt the industry's development, autonomous vehicles should be regulated similarly to how banks and financial institutions are regulated. Because autonomous vehicles are an emerging technology capable of reducing vehicle-related fatalities and injuries, autonomous vehicle technology is "vital"—similar to how banks and financial institutions provide a "vital" service due to the practical and widely-integrated nature of the products and services provided.[84] Data privacy concerns, however, could constitute a barrier to users quickly transitioning from non-autonomous vehicles to partially or fully autonomous vehicles.[85] Because autonomous vehicles have the ability to reduce or eliminate bodily harm,[86] Congress should take steps to speed up the transition by passing data privacy legislation, which would likely calm data privacy concerns. The Gramm-Leach-Bliley Act framework could function as an adaptable template for autonomous vehicle regulation, with appropriate modifications.

78. *See* Kohler & Colbert-Taylor, *supra* note 14, at 120-21.

79. *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1195-96 (2012).

80. *Id.*

81. *See id.* at 1196.

82. *See id.*

83. *See id.* at 1196-97.

84. *See generally* UNION OF CONCERNED SCIENTISTS, *supra* note 6; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 6 at i.

85. *See, e.g.*, United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").

86. *See generally* UNION OF CONCERNED SCIENTISTS, *supra* note 6; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 6 at i.

A. Industry Comparison Among Large Data-Driven Companies, Banks and Financial Institutions, and Autonomous Vehicles

To compare the autonomous vehicle industry with the banking and financial industry, we must rationalize why the law, specifically the Gramm-Leach-Bliley Act, prohibits dissemination of nonpublic personal information by banks and financial institutions to unaffiliated entities after customers opt out, but still allows sharing of such information with affiliated institutions and marketing partners.[87] We must also rationalize why, in particular, banks' and financial institutions' handling of nonpublic personal information is regulated to protect customers' privacy, while large data-driven companies such as Google, Amazon, and Facebook are subject only to self-regulation and are allowed to freely share customer and user data, including nonpublic personal information, with other entities.[88]

1. How Banks and Financial Institutions are Distinguishable from Other Data-Driven Companies

There are three possible reasons why these exceptions and allowances exist under current regulatory regimes: (1) Congress may no longer value customer data privacy surrounding nonpublic personal information, (2) the law simply has not yet adapted to the changing landscape of data usage with the emergence of large data-driven companies, or (3) banks and financial institutions actually provide a distinguishably more vital and integral role in society, and as such warrant use of special regulations. This paper argues that the third possibility provides the true rationalization for why banks and financial institutions are treated and regulated differently than large data-driven companies.

Regarding the first possibility, to explain the lack of sweeping federal legislation on data privacy, we look at the possibility that Congress reversed its expressly stated policy position in favor of protecting individuals' data privacy through the regulation of banks' and financial institutions' handling of customer nonpublic personal information.[89] If Congress *did* in fact reverse its stance on the need for data privacy following the passage of the bipartisan Gramm-Leach-Bliley Act in 1999,[90] we would expect to see at least a partial repeal of privacy statutes related to the financial industry, particularly Sections 6801 through 6809, which refer specifically to the regulation of

87. 15 U.S.C. §§ 6801–6802(b)(2)(2012).

88. *See generally* GOOGLE, *supra* note 73; *see also* AMAZON, *supra* note 73; *Data Policy*, FACEBOOK, *supra* note 73.

89. *See generally* 15 U.S.C. § 6801(a).

90. *See Gramm-Leach-Bliley Act*, CONGRESS.GOV, https://www.congress.gov/bill/106th-congress/senate-bill/900/actions?q=%7B%22search%22%3A%5B%22gramm-leach-bliley%22%5D%7D&r=1&s=3 (last visited Mar. 18, 2019) (passing the Senate by a vote of 90-8, and the House by a vote of 362-57, indicating strong, bipartisan support in the 106th Congress).

financial institutions' handling of nonpublic personal information.[91] Since the Gramm-Leach-Bliley Act (especially the sections related to protecting nonpublic personal information) is still in effect today, we can assume that Congress has not reversed its position on the importance of data privacy.

Regarding the second possibility, to explain the discrepancy between regulations on financial institutions and large data-driven businesses such as Facebook, Google, and Amazon, we consider whether the law has adapted, or will adapt, to the changing nature of online privacy expectations with the emergence of such data-driven companies. As noted, there is no sweeping federal legislation that limits what companies such as Facebook, Google, and Amazon do with the data gathered through business operations.[92] Notably, however, and following the European Union's passage of a much stricter privacy law, the General Data Protection Regulation ("GDPR"), which both standardizes European Union privacy regulations and reinforces individuals' rights in the new era of large data-driven companies,[93] policy drivers in the United States (specifically policy drivers connected to the White House) are for the first time looking to implement "a consumer privacy protection policy that is the appropriate balance between privacy and prosperity."[94] If the United States adopted similar legislation to the GDPR, and if such new legislation also sought to standardize data privacy legislation and created meaningful, enforceable, and actionable data privacy rights in the era of large data-driven companies, data privacy concerns in the autonomous vehicle industry might be alleviated.[95] If no legislation appears in the near future to respond to large data-driven companies' appetite for user data, we must look to the third possibility below.

Finally, regarding the third possibility, to explain why banks' and financial institutions' handling of nonpublic personal information is regulated, while large data-driven companies' handling is not, we look to the nature of the services and products[96] provided by the various players. Large data-driven companies, such as Google, Facebook, and Amazon, offer both products and services.[97] Google offers a range of services, such as search

91. *See* 15 U.S.C. §§ 6801–6809 (2012).

92. *See* David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018), http://fortune.com/2018/11/29/federal-data-privacy-law.

93. *See id.*

94. *See id.*

95. *See, e.g.*, *id.*

96. Referring to services and products available at the date of this writing.

97. *See, e.g.*, *Radically Helpful Things Made By Google*, GOOGLE, https://about.google./products/ [https://perma.cc/V7HB-WFXD] (last visited Mar. 18, 2019); *What Are the Facebook Products?*, FACEBOOK, https://www.facebook.com/help/1561485474074139 [https://perma.cc/4QQ6-2MTE] (last visited Mar. 18, 2019); *Amazon Echo – Black (1st Generation)*, AMAZON, https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa-White/dp/B01E6AO69U [https://perma.cc/XF8Z-VPQ2] (last visited Mar. 18, 2019).

engine access,[98] cloud computing,[99] music services,[100] and much more to specific products, such as phones, tablets, watches, laptops, and more.[101] Facebook offers a social media forum for online interaction and data sharing, and various other products and services.[102] Amazon provides an online marketplace for consumers and sellers to browse, order, and review products and services, as well as other products such as computer hardware and services such as online video streaming.[103]

Each of these companies acquires nonpublic personal information from its users through voluntary information input (such as filling out name, address, and credit card fields), but also through habitual action, such as purchasing behavior, social connections, exchanges of messages, and search terms.[104] Banks and other financial institutions similarly acquire data from voluntary information input (such as name, address, social security number, and more), and can similarly analyze data sets, such as buying behavior, to determine a wealth of additional nonpublic personal information about an individual.[105]

There exists, however, a characteristic of the types of products or services offered that distinguishes banks and financial institutions from large data-driven companies: the widespread and therefore vital nature of the products and services offered to the public.[106] Conversely, there exist meaningful alternatives to using data-driven companies' products (such as using private browsing,[107] "offline shopping," and using other social networking means, such as text messaging or email). Thus, it is then easier to imagine why Congress would want to regulate data privacy for users of a vital service.

2. How Autonomous Vehicles Likewise Drift into Distinguishability

As there has not been any full or partial repeal of the relevant privacy legislation contained in the Gramm-Leach-Bliley Act, it is unlikely that

98. *See generally* GOOGLE, http://google.com [https://perma.cc/P85X-WK3T] (last visited Oct. 9, 2019).

99. *See* GOOGLE, https://blog.google/products/google-cloud/cloud-covered-what-was-new-with-google-cloud-in-september-2019/ [https://perma.cc/FY68-LN4F] (last visited Oct. 9, 2019).

100. *See* GOOGLE, https://play.google.com/music/listen?u=0#/sulp [https://perma.cc/3J6S-EQQJ] (last visited Oct. 9, 2019).

101. *See generally Radically Helpful Things Made By Google*, GOOGLE, *supra* note 97.

102. *See generally* FACEBOOK, https://www.facebook.com [https://perma.cc/LZX3-WSRH] (last visited Mar. 18, 2019).

103. *See generally* AMAZON, https://www.amazon.com [https://perma.cc/DNL7-7AGS] (last visited Mar. 18, 2019).

104. *See* GOOGLE, *supra* note 97; AMAZON, *supra* note 97; FACEBOOK, *supra* note 97.

105. *See* Gertz, *supra* note 58, at 944-46.

106. *See FDIC Survey*, *supra* note 54, at 1.

107. *See, e.g.*, *Browse in Private*, GOOGLE, https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DDesktop&hl=en [https://perma.cc/7AVT-JNC4] (last visited Oct. 13, 2019).

Congress has backtracked on its policy stance on protecting individuals' nonpublic personal information. If the law is soon to adapt to the era of large data-driven companies, like the European Union has with the passage of the GDPR, the autonomous vehicle industry will likely see legislation passed to regulate private companies' handling of nonpublic personal information.[108] If Congress discriminates on industry regulation of data sharing based on the type and value of products and services offered, then the autonomous vehicle industry will also likely see legislation passed both to regulate nonpublic personal information and to reduce any chilling effect that may construct disincentives to autonomous vehicle use. Such legislative action would likely be supported because autonomous vehicles are a similarly vital service due to the fact that the service significantly reduces, or even eliminates, vehicle-related injuries and fatalities.[109]

The argument arises, of course, whether a meaningful alternative would exist to the use of autonomous vehicles. It is true that no Level 4 or above autonomous vehicles (vehicles that do not require human intervention for safe operations) are on the road as of the date of this writing, and thus the obvious meaningful alternative to an autonomous vehicle would be use of a Level 0, 1, 2, or 3 vehicle. It is also true that Level 3 and above vehicles would be able to operate safely in most instances even if there were vehicles on the road operated by humans.[110] While the alternative of driving a Level 0, 1, 2, or 3 vehicle may exist today, as autonomous vehicles become more commonplace in the future, individuals may not need to manually operate a vehicle as frequently as they do today. And as safe driving habits dwindle as time passes, the Level 0, 1, 2, and even some Level 3 alternatives would become less meaningful.

To further explain, as autonomous and self-driving technology continues to integrate into vehicles and as the technology becomes more mainstream, vehicle users will become accustomed to relying on such technology for vehicle operations. This will result in vehicle users losing the safe driving habits required for operation of a Level 0, 1, or 2 vehicle simply because they will not have had the opportunity to practice those habits in a Level 3, 4, or 5 vehicle. This trend would effectively render autonomous vehicle operation (that requires little or no human intervention) vital and widely integrated into society, thereby entitling its users to data protection (at least similar to the minimal protections offered under the Gramm-Leach-Bliley Act,[111] and at most under a new regulatory regime that grants full data protection to autonomous vehicle users).

Simply put, because autonomous vehicles and non-autonomous connected vehicles will reduce or eliminate vehicle-related injuries and

108. *See generally* Meyer, *supra* note 92.

109. *See generally* UNION OF CONCERNED SCIENTISTS, *supra* note 6; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 6 at i.

110. *See* Kohler & Colbert-Taylor, *supra* note 14, at 103; *see also* UNION OF CONCERNED SCIENTISTS, *Self-Driving Cars Explained*, *supra* note 14.

111. *See generally* 15 U.S.C. §§ 6801–6809 (2012).

deaths,[112] autonomous and connected vehicles should be considered vital products and services. The benefits of autonomous and connected vehicles include utilization of technology that (1) enables vehicles to avoid other vehicles, humans, and obstacles,[113] (2) decreases medical expenses from vehicle-related injuries,[114] and (3) reduces traffic congestion through coordinated route-finding.[115] The avoidance of bodily harm through use of autonomous and connected vehicles is just as important as securing individuals' financial privacy in the banking and financial industry, and if Congress sees a legitimate need for data protection in the financial industry, Congress should see an equally, if not more, legitimate need for data protection in the autonomous vehicle industry. And as vehicles continue to increase in autonomy level (from Level 0, 1, and 2 up to Level 3, 4, and 5), driver skill level will decrease as humans relinquish more system management and drive operations to the vehicle's computers.[116]

Indeed, in a fully autonomous vehicle world, the need for driver education may no longer exist, which only increases the vital nature of the autonomous vehicle industry. As for the connected vehicles of today, and the autonomous and connected vehicles of the near future, the immediate benefits of crash avoidance[117] and traffic fatality and injury reduction[118] are sufficient to characterize the autonomous vehicle industry as "vital." Even if the autonomous vehicle industry is not considered "vital," the reasons posed still justify the argument for Congressional passage of legislative regulation to reduce the chilling effect of surveillance capitalism and incentivize autonomous vehicle usage because such vehicles can save lives, reduce vehicle-related injuries, and shorten commutes.[119]

B. The Adaptable Gramm-Leach-Bliley Template

The search for an adaptable regulatory framework brings forth the banking and financial industry. While the Gramm-Leach-Bliley Act may have flaws,[120] it is a good starting point because it regulates the use of nonpublic personal information in an industry fairly analogous to the autonomous vehicle industry.[121] Further, while the "flaws" under the Gramm-Leach-Bliley

112. *See* Juniper Research, *supra* note 26.
113. *See* Mattioli, *supra* note 21, at 279.
114. *See id.* at 279.
115. *See* Amon, *supra* note 3, at 353-54.
116. *See generally* Mich. Dep't of Transp., Impact of Automated Vehicle Technologies on Driver Skills (2016), http://www.cargroup.org/wp-content/uploads/2017/02/IMPACT-OF-AUTOMATED-VEHICLE-TECHNOLOGIES-ON-DRIVER-SKILLS.pdf. [https://perma.cc/DP24-JYAT].
117. *See* Mattioli, *supra* note 21, at 281-82.
118. *See* Juniper Research, *supra* note 26.
119. *See* Amon, *supra* note 3, at 353-54.
120. Such flaws include allowing banks and financial institutions to freely share their users' nonpublic personal information with the institutions' affiliates and marketing partners, even over a user's opt-out.
121. *See generally* 15 U.S.C. §§ 6801–6809 (2012).

Act may not sit well with certain users of banks or financial institutions,[122] the allowances granted by the Act may in fact function to protect the customer. It is possible that such information sharing between banks or financial institutions and their affiliates or marketing partners actually enables the institutions to offer tailored protective services and financial safeguards based on an individual's financial habits.

Thus, this framework would apply well to the autonomous vehicle industry, as the sharing of nonpublic personal information between vehicle manufacturers and their affiliates would be essential to the operation of the vehicle itself due to functions requiring connectivity.[123] Furthermore, sharing nonpublic personal information between autonomous vehicle manufacturers and marketing partners would allow manufacturers to present users with new features of the ever-developing product that best fit, and are most relevant to, the user's preferences and habits. Also, under the adapted Gramm-Leach-Bliley framework, the autonomous vehicle manufacturer would be able to pass along operational data, which would likely include nonpublic personal information,[124] to entities such as Congress, the Department of Motor Vehicles, the National Highway Traffic Safety Administration, and more in order to construct an overall picture of how autonomous vehicles are used, which can in turn provide valuable insight into how to improve the transportation system as a whole. Ideally, autonomous vehicle manufacturers would be willing to share the data with each other in order to work together to create a safer, more comfortable, and more efficient vehicle; however, "such data can give individual automakers a competitive edge,"[125] and is thus unlikely to occur.[126]

Of course, just like under the Gramm-Leach-Bliley Act,[127] autonomous vehicle users should be able to opt out of the information sharing mechanism between manufacturers and unaffiliated entities. As about 95% of customers of banks and financial institutions have declined to opt out under the Act, due to apparent lethargy when faced with the task of altering a default privacy setting,[128] it is possible that a similar percentage of autonomous vehicle users would also decline to opt out of the data sharing mechanism, which would allow regulatory bodies and transportation and safety entities to analyze data to research and implement system-wide improvements.

Thus, to maximize transportation safety, while incorporating data privacy concerns, Congress should legislate the use of vehicle data to allow a larger group of individuals, both data privacy-apathetic and data privacy-concerned, to enjoy the many benefits of autonomous vehicles.

---

122. *See* Gertz, *supra* note 58, at 983-84.
123. *See* Amon, *supra* note 3, at 342.
124. *See* Mattioli, *supra* note 21, at 288.
125. *Id.* at 279.
126. *See id.*
127. *See* 15 U.S.C. § 6802(b) (2012).
128. *See* McClurg, *supra* note 70, at 135.

IV. PROPOSED SOLUTION: "P.A.V.E.R."

Regulatory legislation passed by Congress is essential to deconstruct barriers to connected vehicle use (by avoiding the chilling effects of surveillance capitalism on purchases of such vehicles), similar to those possibly obstructing society's full embrace of the autonomous vehicle industry, so that more consumers buy vehicles with vehicle-to-vehicle ("V2V") capacity, which will in turn result in an increase in lives saved and injuries avoided.[129]

A. How the Adapted Gramm-Leach-Bliley Regulation ("P.A.V.E.R.") Would Work with the Autonomous Vehicle Industry

If Congress chooses not to pass sweeping federal privacy laws, similar to the General Data Protection Regulation in the European Union, and the U.S. maintains its current patchwork framework for data privacy regulation, Congress should implement an adapted Gramm-Leach-Bliley regulatory regime to the autonomous vehicle industry that focuses on the protection of users' nonpublic personal information. The proposed statutory regulation, which could be called the Privacy in Autonomous Vehicles and Enforcement Regulation, or "P.A.V.E.R.," would closely mirror the Gramm-Leach-Bliley Act, as codified under 15 U.S.C. §§ 6801–6809.[130] The purpose of P.A.V.E.R. would be to safeguard vehicle users' nonpublic personal information, while still allowing for fully functional operation of the vehicle to the extent necessary to reduce or eliminate bodily harms caused by vehicles.

Section 1 of P.A.V.E.R. would outline Congress's policy stance regarding the need to protect autonomous vehicle users' nonpublic personal information. It would also outline the unambiguous reasons for implementing P.A.V.E.R., including, similar to the Gramm-Leach-Bliley Act, the need to protect the "security and confidentiality of customer records and information," the need to "protect against any anticipated threats or hazards to the security or integrity of such records," and the need to "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[131]

Section 2 of P.A.V.E.R. would outline the vehicle manufacturers' disclosure obligations regarding data sharing policies. This provision would operate similarly to the corresponding Gramm-Leach-Bliley section in that manufacturers must provide notice of their sharing practices of users' nonpublic personal information with the manufacturers' marketing partners, affiliates, and other unaffiliated third parties in order to promote the manufacturers' business interests.[132] Just like in the Gramm-Leach-Bliley

129. *See* Juniper Research, *supra* note 26.
130. *See generally* 15 U.S.C. §§ 6801–6809 (2012).
131. *Id.* §§ 6801(b)(1)–6801(b)(3) (2012).
132. *See id.* § 6802.

Act,[133] if the vehicle user wishes to limit sharing of his or her own nonpublic personal information, Section 2 of P.A.V.E.R. would contain an opt-out mechanism (which must be clearly communicated to the customer) whereby the manufacturer must cease sharing that user's nonpublic personal information with unaffiliated third-party entities. Different from the operation of the corresponding Gramm-Leach-Bliley Act provision, [134] under P.A.V.E.R., the manufacturer must also cease sharing nonpublic personal information with affiliates and marketing partners. Note, however, that, § 6802(e) of the Gramm-Leach-Bliley Act also does not prohibit disclosing nonpublic personal information to unaffiliated third-party entities if it is "necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with . . ."[135] other services offered or maintaining or servicing the vehicle's hardware or software.[136] As such, similar to that corresponding provision,[137] such data sharing would be allowed if it proves essential to the vehicle's fundamental operation as outlined by the rulemaking bodies in Section 4 of P.A.V.E.R.[138] This is necessary to close the loophole in the Gramm-Leach-Bliley Act that can be exploited by some banks and financial institutions that allow such institutions to simply designate certain entities as "marketing partners" and continue business as usual. Further, and different from the Gramm-Leach-Bliley Act, this statute would also prohibit any downstream manufacturers or entities engaged in pre-sale handling of the vehicle from installing data collection devices or software, but would not prohibit aftermarket alterations. This section would additionally apply to domestic importation of autonomous or connected vehicles manufactured or handled by foreign entities, if the vehicles are intended for sale, or are actually sold, in the United States.

Section 3 of P.A.V.E.R. would set forth a requirement for autonomous vehicle manufacturers, at the time of the establishment of a customer relationship, to disclose to the customer the data privacy policy implemented in the vehicle, similar to the corresponding Gramm-Leach-Bliley provision.[139] This provision is necessary to ensure that the buyer is fully informed.

Section 4 of P.A.V.E.R., again, similar to the corresponding provision in the Gramm-Leach-Bliley Act,[140] would set forth the rulemaking power of the relevant federal agencies and administrations. Here, the Federal Trade Commission shall have the authority to prescribe such regulations as may be necessary to carry out the purposes of this subtitle with respect to any autonomous or connected vehicle manufacturer, as well as pre-sale entities that handle such vehicles. Notwithstanding the authority of the Federal Trade Commission, the Department of Transportation (and specifically the National

133. *See id.*
134. *See id.*
135. *Id.* § 6802(e).
136. *See id.*
137. *See id.*
138. *See, e.g.*, *id.*
139. *See* 15 U.S.C. § 6803 (2012).
140. *See id.* § 6804.

Highway Traffic Safety Administration, because it is an enforcement agency dedicated to avoiding bodily harm "through enforcing vehicle performance standards and partnerships with state and local governments"[141]) shall have the authority to prescribe such regulations as may be necessary to carry out the purpose of this subtitle with respect to any autonomous or connected vehicle manufacturer.

Section 5 of P.A.V.E.R., like the corresponding Gramm-Leach-Bliley Act provision,[142] would handle enforcement. The Federal Trade Commission and the Department of Transportation (especially the National Highway Traffic Safety Administration) shall enforce the regulations adopted pursuant to the statute generally. The U.S. Customs and Border Protection office will have the authority to inspect any imported autonomous or connected vehicles to ensure that such vehicles are imported by foreign manufacturers or other foreign entities that both have import permits and are certified to distribute vehicles in compliance with P.A.V.E.R.

Section 6 of P.A.V.E.R. would outline how P.A.V.E.R. interacts with other federal and state laws. Section 6 would also combine two sections in the Gramm-Leach-Bliley Act that correspond with this subject matter. In particular, just like the corresponding Gramm-Leach-Bliley provision, P.A.V.E.R. would only supersede inconsistent state laws, not more restrictive regulations.

Finally, Section 7 of P.A.V.E.R. would include relevant definitions, including, for example, the definition of a "manufacturer," and the definition of the terms "connected" and "autonomous" as they relate to vehicles.

B. Other Proposed Solutions to Data Privacy Issues

There are some legal scholars that view the Gramm-Leach-Bliley Act as insufficient to protect consumers' data privacy concerns.[143] Some call for a change to the Act's data sharing framework, and would prefer that consumers be opted-out of data sharing by default, rather than the Act's current default where customers are opted-in,[144] in order to avoid interfaces "deliberately designed to deter people from exercising their rights."[145] In fact, there is discussion by some scholars that collecting and selling "an extensive consumer data profile without consumer consent should be actionable under the privacy tort known as appropriation."[146] This notion, however, appears not to be explicitly supported by Congress as is evidenced both by the Gramm-Leach-Bliley Act's allowance of disseminating information under certain circumstances, even with customer opt-out,[147] and by the lack of

141. *The National Highway Traffic Safety Administration is Responsible for Keeping People Safe on America's Roadways*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/about-nhtsa [https://perma.cc/K8Q4-N252] (last visited Oct. 9, 2019).

142. *See* 15 U.S.C. § 6805 (2012).

143. *See, e.g.*, McClurg, *supra* note 70, at 133-37.

144. *See id.*

145. *See id.* at 135.

146. *See id.* at 69.

147. *See* 15 U.S.C. § 6802(b) (2012).

legislation pertaining to data use by large data-driven companies such as Google or Facebook.[148] Still, other legal scholars believe that data collection for online profiling (especially for targeted advertising purposes) constitutes an invasion of privacy that falls under a different privacy tort.[149] There has been no enforcement in the federal courts, however, of such proposed policies (although there is some state legal action towards this effect).[150] This evidence, as applied to the autonomous vehicle industry, indicates that it is unlikely, under today's common law or statutory framework, that autonomous vehicles would be subjected to a stricter data handling standard than large data-driven companies, which is why P.A.V.E.R. is needed.

More specific to the autonomous vehicle industry, there is actually some evidence that Congress previously split in its policy position on how to handle data sharing with connected vehicles.[151] This is evidenced by prior (but failed) Congressional consideration of conflicting legislation: one bill to "allow drivers to opt-out of vehicle location tracking altogether,"[152] and another bill that would "require mandatory data-sharing between automakers"[153] in order to streamline collision avoidance.[154] It seems obvious that *some* location tracking would be necessary for the products to function properly and to navigate the vehicle from one location to another. Thus, a complete opt-out of vehicle location tracking seems counterproductive to the goal of autonomous transportation. Conversely, if there was a statutory requirement for data sharing between automakers, competition could be dampened between manufacturers,[155] resulting in heavier scrutiny of the vehicle data in an attempt to analyze customer data to more effectively promote products,[156] which can ultimately lead to the chilling effect on individuals' freedoms of expression and association that Justice Sotomayor discussed in *United States v. Jones*.[157] P.A.V.E.R. would remove this chilling effect by allowing users to opt out of data sharing for marketing purposes, but compromise by allowing some data sharing for vehicle operation purposes.

Other legal scholars discuss the idea that connected and autonomous vehicle manufacturers should be forced to install the ability to interact with a portal that allows users to read manufacturers' privacy statements and either opt in or opt out of data sharing directly from the screen.[158] This solution to data privacy concerns is problematic because it substantially infringes on manufacturers' design autonomy. Rather than legislating the means by which users can interact with vehicles, Congress should legislate how manufacturers

148. *See* Meyer, *supra* note 92.
149. *See, e.g.*, Gertz, *supra* note 58, at 1004-05.
150. *See* Meyer, *supra* note 92.
151. *See* Mattioli, *supra* note 21, at 280.
152. *Id.*
153. *Id.*
154. *See id.* at 279.
155. *See id.* at 295.
156. *See id.* at 279.
157. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *see also* Mattioli, *supra* note 21, at 293.
158. *See* Amon, *supra* note 3, at 360-61.

handle nonpublic personal information while, importantly, allowing manufacturers the freedom to design an optimal vehicle that complies with the regulation. No matter the regulatory approach, the need for relevant data privacy law (whether common law or statutory regulation) is a prevailing element of many of the other proposed solutions both to the autonomous vehicle data privacy issue and to the perceived shortcomings of the Gramm-Leach-Bliley Act.[159]

V. CONCLUSION

Overall, there are still several questions that must be answered to provide an adequate solution to the issue of connected and autonomous vehicle data privacy. First, society must decide how much weight to give to data privacy concerns, which must then be adopted by Congress in order to accurately represent that societal stance. Although many privacy scholars and data experts have written on the issue, if society, for the most part, is not as concerned with data privacy as the experts are, then data privacy regulations may be largely unnecessary. Second, the issue of timing must be addressed. Although vehicle manufacturers are in the process of rolling out autonomous vehicles,[160] transportation users are not yet heavily exposed to such vehicles, and may not yet feel that the sanctity of their nonpublic personal information is truly compromised. Conversely, connected vehicles capable of similar data collection are increasingly prevalent in society.[161] Although some may see the issue of vehicle-related data privacy as an issue for the future, careful monitoring of the industry's progress is necessary to decide when regulation is needed, and allowing ample time to formulate and pass such regulations must be taken into account.

Nonetheless, just as commerce and financial security would likely crumble without banks, so too would future transportation systems suffer from increased dependency on autonomous features without autonomous vehicles. As such, both the financial industry and the autonomous vehicle industry qualify as vital industries (especially in the near future), but only the financial industry has regulation that deconstructs barriers to use. While financial security is extremely important, so too is the avoidance of bodily injury and death due to autonomous vehicles' superior safety capabilities. Further, as is discussed in the introduction,[162] individuals must have the ability to control how vital industry entities, such as autonomous vehicle manufacturers, use their nonpublic personal information in order to streamline

159. *See generally* Mattioli, *supra* note 21, at 277-98; Glancy, *supra* note 79, at 1171-1239; McClurg, *supra* note 70, at 63-143; Gertz, *supra* note 58, at 944-1018; Amon, *supra* note 3, at 329-61; Kohler & Colbert-Taylor, *supra* note 14, at 100-38.

160. *See, e.g.*, Giambrone, *supra* note 16.

161. *See* Juniper Research, *supra* note 26.

162. *See supra* Section I.

the transition to "safer, smarter, and more efficient roadways."[163] Thus, the roads of the future require P.A.V.E.R.

163. *See* Amon, *supra* note 3, at 361.