1-1-2017

Who's Driving You? Driver Data Remains Unprotected Under COPPA and Shine the Light

Marisa Tashman
Loyola Law School, Los Angeles

WHO'S DRIVING YOU? DRIVER DATA REMAINS UNPROTECTED UNDER COPPA AND SHINE THE LIGHT

Marisa Tashman∗

As our lives become more driven by technology, California's privacy laws fall short of protecting our personally identifiable information. Vehicles in particular present an increasing privacy concern, as our automobiles become more computer and less car. Cars today have increasingly sophisticated capabilities, stemming from connected technology and sensors, and their ability to capture geolocation and biometric data. This data can be used to make inferences about drivers' behavioral patterns and daily habits. This Article analyzes whether California's privacy laws—California Online Privacy Protection Act ("COPPA") and Shine the Light—adequately address privacy concerns regarding driver data collected by the connected car. This Article considers how notice and consent can effectively protect connected car drivers, and concludes that consumers need a more effective way to manage how connected car data is collected, retained, and used.

∗ J.D., 2017, Loyola Law School, Los Angeles; B.A. Sociology, 2012, Brandeis University. Thank you to Professor John Nockleby for providing me with guidance and inspiration. I also want to thank Professor Karl Manheim, Professor Lauren Willis, the *Loyola of Los Angeles Law Review* editorial board and staff, and Damien Amey for spending countless hours reading through my article and providing me with additional feedback.

TABLE OF CONTENTS

I. INTRODUCTION

Sit down, get comfortable. Your seat recognizes you, adjusts to the perfect amount of lumbar support. Your breathing patterns are noticed, and your heartbeat is recorded—you are remembered. You are running late, and you are anxious. Your Pandora application begins to play the music you listen to when you need to calm down. Suddenly a pop-up appears on the screen in front of you—"Remember to relax." You click "Dismiss" and breathe. You wonder if you have time to pick up lunch before your meeting. Another pop-up opens on the screen. The new sandwich shop you read about on Yelp! is on the way. You click "GO," buckle your seatbelt, and put the car in drive. You are about to pull out of your parking spot when you are interrupted by a loud "BEEP." In the corner of your eye, you see an orange hazard light on your side mirror. Another car zooms past. This is the connected car.

Each year cars[1] become more computer and less car. Although vehicles have relied on computers for almost three decades in systems such as the electronic throttle, braking, and steering,[2] cars today have increasing capabilities stemming from connected technology and sensors. The connected car refers to "the use of in-car telematics, a range of technologies that leverage connectivity, whether over the internet or via dedicated short-range communications (DSRC), with diagnostic, location, or other information to provide new safety, convenience, and communications services."[3] The connected car's "information networks are created through wired and wireless communications technologies embedded in physical objects."[4] The connected car gathers behavioral and personalized data, capturing "incredibly rich nuance[s] about who we are, how we behave, what our tastes are, and even our intentions."[5] For example, vehicles can

1. This Article focuses on personal vehicles, not vehicles used in a commercial context.

2. FUTURE OF PRIVACY FORUM, THE CONNECTED CAR AND PRIVACY: NAVIGATING NEW DATA ISSUES 2 (2014), http://www.futureofprivacy.org/wp-content/uploads/FPF_Data-Collection-and-the-Connected-Car_November2014.pdf.

3. *Id.* at 5.

4. Comments on Connected Smart Technologies in Advance of the FTC "Internet of Things" Workshop, from the Future of Privacy Forum, to the U.S. Federal Trade Commission 3 (May 31, 2013) [hereinafter Future of Privacy Forum Comments], https://fpf.org/wp-content/uploads/FPF-Comments-Regarding-Internet-of-Things.pdf.

5. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 90 (2014); *see also* Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. 205, 210 (2014) ("One of the most troubling risks coming from the collection and use of big data is its use in making sensitive predictions about consumers, such as those

sense nearby vehicles and warn drivers of vehicles in the lanes next to them.[6] Cars also have sophisticated multimedia systems that instantly provide drivers with information on weather, stocks, and news.[7] In the not-so-distant future, cars will be able to communicate and exchange data with nearby vehicles and infrastructure[8] to improve roads, traffic, and driver safety.[9]

Along with the great benefits of the connected car come significant privacy concerns regarding the collection, storage, and use of drivers' behavioral and personal data.[10] Connected cars collect data regarding driving behavior such as braking and accelerating patterns, steering habits, speed, and seatbelt usage.[11] Connected cars also collect location data and data used by third-party applications in their infotainment systems.[12] Onboard sensors obtain information about a vehicle's surroundings, such as detecting lane markings and obstacles.[13] Technological advances will soon permit connected cars to collect drivers' breathing patterns using seatbelt sensors and heart rates using steering wheel sensors, and will also be enabled with facial recognition capabilities.[14] Data collected by the connected car can be used to make inferences about drivers' behavioral patterns and daily

involving their health conditions, sexual orientation, religion, and race.").

6. *See, e.g.*, *2016 GX Safety*, LEXUS, http://www.lexus.com/models/GX/safety (last visited Sept. 21, 2015) (featuring intelligent high-beam headlamps, blind spot monitor, and lane departure alert); *Safety*, MERCEDES-BENZ, http://www.mbusa.com/mercedes/benz/safety (last visited Sept. 21, 2015) (featuring attention assist, active blind spot assist, and active lane keeping assist).

7. *Lexus Enform: App Suite*, LEXUS, http://www.lexus.com/enform/#app-suite (last visited Sept. 20, 2015); *Ford SYNC, SYNC AppLink*, FORD, http://www.ford.com/technology/sync/ (last visited Oct. 20, 2015).

8. Infrastructure includes roadside infrastructure such as traffic lights, lane markers, roadside barriers, and buildings. Dorothy J. Glancy, *Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J.L. SCI. & TECH. 619, 644 n. 69 (2015) [hereinafter Glancy I]; *see also* Dorothy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J. 1617, 1626 (2014) [hereinafter Glancy II].

9. Future of Privacy Forum Comments, *supra* note 4, at 11–12 ("City planners and departments of transportation should be able to use aggregate driving information to optimize traffic flows and identify roads in need of repair.").

10. *See* Glancy II, *supra* note 8, at 41 ("Information privacy concerns about potential misuse of this personal information are likely to range from opposition to the collection of personal information so that it can be sold or traded, to restrictions against use of information in behavioral advertising.").

11. FUTURE OF PRIVACY FORUM, *supra* note 2, at 5, 9.

12. *Id.* at 8–9; *see also Lexus Enform: App Suite*, *supra* note 7 (showing the variety of applications accessible within Lexus vehicles).

13. FUTURE OF PRIVACY FORUM, *supra* note 2, at 8.

14. *Id.* at 8–9.

habits.[15] Access to this meaningful data, therefore, leads to great privacy concerns, including data being sold to third-party marketers,[16] data being used by insurance companies to evaluate claims and set premiums,[17] as well as data being accessed by criminal hackers.[18]

While the connected car implicates privacy concerns that are both national and international in scope, this issue is particularly pressing in California. California is the world's eighth largest economy, home to more than thirty-eight million consumers and twenty-four million drivers.[19] If online service or website operators want to do business in California, they must comply with the state's privacy protection laws as they apply to every business that collects information about Californians via its website.[20] Thus, the impact of California's privacy laws extends far beyond the state's borders.[21]

California is one of the few states that has a constitutional right to privacy.[22] Article I of the state's constitution provides: "All people are by nature free and independent and have inalienable rights. Among

15. Peppet, *supra* note 5, at 121–22.

16. Glancy II, *supra* note 8, at 1639, 1658.

17. FUTURE OF PRIVACY FORUM, *supra* note 2, at 4. *See generally* Peppet, *supra* note 5, at 118 ("Employers, insurers, lenders, and others may then make economically important decisions based on those inferences, without consumers or regulators having much understanding of that process.").

18. Glancy II, *supra* note 8, at 1661 ("According to GAO, security of connected vehicle communications and networks poses one of the most serious unresolved challenges for both safety and mobility types of connected vehicles."); *see also* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (Jul. 21, 2015), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (The author describes his experience participating in an experiment with two hackers who remotely took control of his Jeep. This was the first time hackers remotely gained access to a vehicle. They were able to completely take control of the car, cutting the transmission and the brakes, manipulating the radio, controlling the air conditioning, and blurring the windshield with wiper fluid.).

19. CAL. DEP'T OF JUSTICE, CALIFORNIA DATA BREACH REPORT i (2014); *Total Number of Licensed Drivers in U.S. in 2013, By State*, STATISTA (2015), http://www.statista.com/statistics/198029/total-number-of-us-licensed-drivers-by-state/ (last visited Nov. 13, 2015).

20. Gregory James Evans, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 205 (Winter 2015).

21. *Id.*

22. *See Privacy Protections in State Constitutions*, NAT'L CONFERENCE OF STATE LEGISLATURES (Dec. 12, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (showing a table of the ten states with privacy protection provisions in their constitutions); *see also* ALASKA CONST. art. I, § 22 (2015); ARIZ. CONST. art. II, § 8 (2015); CAL. CONST. art. I, § 1 (Deering 2015); FLA. CONST. art I, § 23 (2015); HAW. CONST. art. I, § 6 (2015); ILL. CONST. art. I, § 6 (2015); LA. CONST. art. I, § 5 (2015); MONT. CONST. art. II, § 10 (2015); S.C. CONST. art I, § 10 (2015); WASH. CONST. art I, § 7 (LexisNexis 2015).

these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[23] This right to privacy has woven its way into consumer-focused policies and legislation, contributing to California's leadership in consumer privacy rights.[24] In 2003, California became the first state to mandate data breach notifications,[25] requiring businesses and state agencies to alert Californians when a security breach has exposed their personal information.[26] The California Department of Justice's Privacy Enforcement and Protection Unit is dedicated to guiding businesses, organizations, and government entities on how to comply with the California Online Privacy Protection Act ("COPPA").[27] Despite California's leadership in consumer privacy, the state has failed to adequately address privacy concerns regarding driver data collected by the connected car.

The connected car's features increase convenience, entertainment, and driver safety, but they also collect vast amounts of behavioral and sensor data.[28] Although this data may initially be de-identified, Big Data technologies[29] can undo de-identification to

23. CAL. CONST. art. I, § 1 (Deering 2015).

24. "In 2013 alone, the state legislature enacting six significant privacy and data security bills…In a single year, the California legislature enacted six bills which address privacy, data security, and a combination of the two." Evans, *supra* note 20, at 206. California enacted a breach notification law in 2002 and in 2013, expanded the types of personally identifiable information included. CAL. CIV. CODE §§ 1798.29, 1798.82 (Deering 2013). In 2014, California required websites to disclose how they respond to browser-based "do not track" requests. CAL. BUS. & PROF. CODE § 22575 (Deering 2013). The state also leads the country in laws securing medical information on mobile applications as well as information collected by utility companies. CIV. § 56.06 (regarding confidentiality of medical information in mobile applications); *id.* § 1798.98 (regarding privacy and security of gas and electrical usage data).

25. CAL. DEP'T OF JUSTICE, *supra* note 19, at i.

26. California's Data Breach Notification Law requires organizations, businesses, and government agencies who maintain customer's personal information to notify California residents when their data was acquired by an unauthorized person. The notification must include the types of information compromised, a general description of the breach, and an offer for identify theft prevention and mitigation. "Personal information" includes an individual's name plus one of the following: social security number, driver's license number, financial account information, medical information, and health insurance information. This law's 2014 amendment to include information "maintained," not just owned or licensed, by a business, expands the scope of the law to mandate disclosure of a breach even when the data is not directly owned by the source of the breach. CAL. CIV. CODE §§ 1798.29, 1798.82, & 1798.84 (Deering 2015).

27. *Office of the Attorney General, Privacy Enforcement and Protection*, ST. OF CAL. DEP'T OF JUSTICE, http://oag.ca.gov/privacy (last visited Sept. 20, 2015); *see also* CAL. BUS. & PROF. CODE §§ 22575–579

28. Glancy I, *supra* note 8, at 634–38.

29. *See infra* Section II(A)(5).

understand drivers' habits and behaviors.[30] This becomes a danger to individual privacy because the definition of personal information in California privacy laws excludes de-identified data, even if that data can later become identified. The connected car extends drivers' relationships with their vehicles to include communications and online connectivity, but the fundamental nature of a car as a private space does not change. Drivers are unaware of the potential threat to their personal privacy, and automakers gain valuable information from driver data without being legally required to disclose their data practices or give drivers a choice in whether their data is collected and shared. The privacy policies for the connected car's features, many run by third parties, are separate, and it is unreasonable to expect consumers to read or understand them all.[31] Even if consumers took the time to read and understand them, they would have no option to opt out of data collection by certain features unless they gave up the features altogether.[32] Drivers would also remain unaware of exactly who was using, selling, or analyzing their data.[33] This privacy issue escalates as connected cars become driverless cars, with drivers giving up more of their data as the technologies become further advanced.[34] By expanding the definition of personally identifiable information in COPPA and Shine the Light to include behavioral and sensor data collected by the connected car, automakers and third-parties in this industry would be required to grant drivers notice and consent

30. William J. Kohler & Alex Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles*, 31 SANTA CLARA COMPUTER & HIGH TECH. L.J. 99, 120–21 (2015) ("Even if this data is scrubbed of unique individual identifying markers…data-mining techniques will almost certainly be able to reconstruct personal identifying information about particular vehicles and by extension their regular occupants."); *see also* BC FREEDOM OF INFORMATION AND PRIVACY ASS'N, THE CONNECTED CAR: WHO IS IN THE DRIVER'S SEAT? 65 (2015), https://fipa.bc.ca/wordpress/wp-content/uploads/2015/05/CC_report_lite-1v2.pdf [hereinafter FIPA Report] ("Data analytics takes aggregate data about consumers and combines it in ways that reveal particular things about individuals (e.g., our habits, preferences, interests, social circles) that the individual might wish to keep private. On the basis of aggregate data, analytics can then make remarkably accurate predictions of individual behavior, allowing corporations (or governments) to categorize individual consumers by behavioural profile and target them for marketing or other purposes.").

31. Adam Thierer, *Privacy, Security, and Human Dignity in the Digital Age: The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 446–47 (2013).

32. *See infra* Section III(B)(4).

33. *See infra* Section III(B).

34. Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 WAKE FOREST J. L. & POL'Y 339, 382 (June 2015); Glancy I, *supra* note 8, at 676.

opportunities regarding how their data is collected, used, and disclosed.

This Article analyzes the inadequacies within COPPA and Shine the Light as applied to the connected car. More specifically, it demonstrates that the definition of personal information is underinclusive, as it leaves vast amounts of data collected by the connected car exposed and unprotected. Part II of this Article provides information on connected car technologies and summarizes COPPA and Shine the Light. Part III discusses the shortcomings within COPPA and Shine the Light, focusing on each statute's definition of personal information and related exemptions. Part IV focuses on potential solutions and argues to expand the definition of personal information to include behavioral and sensor data collected by the connected car. Moreover, Part IV considers how notice and consent can effectively protect connected car drivers. Part V concludes that consumers need a more effective way to manage how connected car data is collected, retained, and used. Furthermore, it urges the California legislature and policymakers statewide to reconsider what type of information is considered personally identifiable.

II. BACKGROUND

This section provides an overview of connected car technologies that give rise to personal privacy concerns in the legal framework of COPPA and Shine the Light. While these technologies increase driver comfort, convenience, and connectivity, technology's advancement depends on collecting and processing vast amounts of driver data, leading to increased privacy concerns.

A. Connected Car Technology: How Drivers' Information Is Collected and Used

Computerized systems were installed in cars as early as 1969.[35] Computerized ignition control and fuel injection systems gained popularity in the 1970s in the midst of the gas crisis when Congress passed new emissions mandates.[36] In the early 1990s, on-board diagnostics ("OBDs") became standard[37] to process the fuel mixture

35. FUTURE OF PRIVACY FORUM, *supra* note 2, at 2.

36. Eli Laurens, *Car Computer History*, EHOW, http://www.ehow.com/about_5082250_car-computer-history.html (last visited Sept. 19, 2015).

37. FUTURE OF PRIVACY FORUM, *supra* note 2, at 2.

and timing and also to control other electrical processes, including climate, brakes, and the odometer.[38] Computer chips and electronic components beyond OBDs are now the norm, "increasing the data volume produced by a car,"[39] and leading to privacy concerns over that data. The main mechanisms of connected car data collection are outlined below.

1. Infotainment Systems

Infotainment systems,[40] increasingly common in new cars, enable drivers to access an array of applications and connect to a driver's cell phone via Bluetooth.[41] Infotainment systems "generate data about the information and entertainment content choices of system users, their use of mobile applications and concierge services, their web browsing activity, social networking, voice, text, and email communications from the car," as well as personal contacts and calendar data.[42] Infotainment systems enable drivers to utilize apps such as OpenTable and Yelp!, have hands-free phone calls, read and answer text messages and emails, and check the weather—all from within the car, without looking at a cell phone.[43] These systems may require a subscription in which the automaker or service provider would store personal information such as name, address, and payment information.[44]

Privacy concerns arise because these systems collect and share a broad range of information, from passwords and payment information, to frequented restaurants, location data, and the contacts stored in a driver's phone.[45] Drivers may not understand how the applications capture their information or with which third parties their data is shared.[46] Data generated by infotainment systems "can be highly revealing of an individual's personal life, values, interests, and

38. Laurens, *supra* note 36.

39. FUTURE OF PRIVACY FORUM, *supra* note 2, at 2.

40. Infotainment systems enable the vehicle to connect to the internet in order to use various services and applications and typically include a dashboard interface and a voice recognition system allowing drivers to engage in hands-free operation. FIPA Report, *supra* note 30, at 24.

41. FUTURE OF PRIVACY FORUM, *supra* note 2, at 7.

42. FIPA Report, *supra* note 30, at 60.

43. FUTURE OF PRIVACY FORUM, *supra* note 2, at 7; *see, e.g.*, *Lexus Enform: App Suite*, *supra* note 7; *Connected Drive*, BMW, http://www.bmwusa.com/standard/content/innovations/bmwconnecteddrive/connecteddrive.aspx#view_apps (last visited Sept. 21, 2015).

44. FUTURE OF PRIVACY FORUM, *supra* note 2, at 10

45. *Id.* at 9–10; Glancy II, *supra* note 8, at 1658; *see* FIPA Report, *supra* note 30, at 60.

46. Glancy II, *supra* note 8, at 1657.

preferences."[47] Not only can this information be used by third-party marketers for advertising purposes,[48] it can also be used "to profile, target[,] and discriminate among individuals in unacceptable ways."[49]

2. Event Data Recorders

Event Data Recorders ("EDRs"), often referred to as a vehicle's "black box,"[50] capture a brief snapshot of information related to an event, like a car crash.[51] EDRs collect vehicle information such as speed, braking patterns, steering, and airbag deployment.[52] EDRs also collect occupant information like seatbelt usage.[53] This data is recorded for a brief period before, during, and after a crash.[54] Unlike other data collected by the connected car, EDR data is not remotely transmitted outside the car and is only retrieved via direct access by a technician, requiring physical access to the vehicle[55] and the owner's consent.[56] About ninety-six percent of new cars in the United States contain an EDR.[57] The National Highway Traffic Safety Administration ("NHTSA") does not limit the types of data that EDRs collect nor does it specify who owns the data or whether it can be used by third parties.[58] Automakers, therefore, have free range to broaden the scope of the data collected, including information such as seat positions, occupant size, vehicle location, and phone or radio usage.[59]

47. FIPA Report, *supra* note 30, at 64.
48. Kohler & Colbert-Taylor, *supra* note 30, at 121–22.
49. FIPA Report, *supra* note 30, at 64.
50. Peppet, *supra* note 5, at 91.
51. FUTURE OF PRIVACY FORUM, *supra* note 2, at 3.
52. *Id.*; *see also* Peppet, *supra* note 5, at 104–05 ("The NHTSA [(National Highway Traffic Safety Administration)] requires that EDRs collect fifteen types of sensor-based information about a car's condition, including braking status, vehicle speed, accelerator position, engine revolutions per minute, safety-belt usage, air-bag deployment, and number and timing of crash events . . . . The NHTSA requires that EDRs store such information for thirty seconds after a triggering impact, thus providing a composite picture of a car's status during any crash or incident.").
53. Peppet, *supra* note 5.
54. *Id.*
55. FUTURE OF PRIVACY FORUM, *supra* note 2, at 3.
56. CAL. VEH. CODE § 9951(c) (Deering 2015).
57. FUTURE OF PRIVACY FORUM, *supra* note 2, at 3.
58. Peppet, *supra* note 5, at 105.
59. *Id.*

3. On-Board Diagnostics

OBD ports are a standard piece of hardware located near the steering wheel, under the dashboard.[60] OBDs collect data regarding vehicle emissions, tire pressure, mileage, time to next oil change, and GPS information.[61] OBD data provides simplified ways for technicians to diagnose problems, and drivers can be notified of such problems through engine check notification lights.[62] Insurance companies also use OBD data to provide safe driver programs and personalized rates.[63] Telematics now enables OBD data to be sent wirelessly to off-board computers that store and process the data into usable information.[64] This information is stored in the cloud, accessible without physically connecting to the car, thus making data readily available and easy to process by automakers and authorized third parties.[65]

The privacy concerns are far greater with OBDs than with EDRs.[66] OBDs record more diverse types of information and store that information for longer periods of time, whereas EDRs only capture data in the moments surrounding a car crash.[67] Because OBD data is stored over time, those with access to that data can conclude

60. FIPA Report, *supra* note 30, at 22–24.

61. *Id.*

62. FUTURE OF PRIVACY FORUM, *supra* note 2, at 4.

63. *Id*. For example, Metromile, a start-up car insurance company based in California, measures rates according to miles driven by connecting their Pulse product to the vehicle's OBD port. Metromile also collects location information, alerts drivers when they are parked in a street cleaning zone, helps drivers optimize fuel usage, and educates drivers about the health of their engine. *Insurance*, METROMILE, https://www.metromile.com/insurance/ (last visited Oct. 2, 2015). Progressive Snapshot, not yet available in California, is an example of a "pay how you drive" program which calculates rates based on risky driver behavior, such as hard-braking or quickly accelerating while also taking into account distance driven. *Snapshot*, PROGRESSIVE, https://www.progressive.com/auto/snapshot/ (last visited Sept. 20, 2015).

64. FIPA Report, *supra* note 30, at 22–24. For example, consumer products geared toward increasing drivers' understanding of how they drive connect to the OBD port and sync that data through a Bluetooth connection to the driver's cell phone. Peppet, *supra* note 5, at 105. The Automatic Link, for example, collects data such as braking and acceleration patterns, GPS location data, engine data, and fuel data to enable drivers to understand how efficiently their engine is running, optimize their fuel usage, and decode engine problems. *The Automatic App*, AUTOMATIC, https://www.automatic.com/features/ (last visited Oct. 2, 2015).

65. Peppet, *supra* note 5, at 106; *see also* FIPA Report, *supra* note 30, at 29 ("Cloud computing is the distribution of computing tasks over several servers and other computer equipment so as to make efficient use of computer resources. Rather than each company using its own server to store and analyze data, several companies can pool server resources so as to provide faster and more reliable access to stored data.").

66. FIPA Report, *supra* note 30, at 24.

67. Peppet, *supra* note 5, at 106.

information about driver habits and patterns.[68] These patterns draw a picture of an individual's life, such as what time the driver leaves and comes home each day, the routes he takes, whether he is an aggressive or passive driver, and how often he drives.[69]

4. Additional Sensor Systems

Other sensor systems that collect various types of data to increase safety and improve the driving experience are standard in connected cars. Internal sensors can obtain information about physical or biological characteristics of a driver.[70] For example, conductive sensors in the steering wheel can measure pulse and body temperature, allowing the car to detect the driver's comfort level and adjust the climate accordingly.[71] Sensors in the seatbelt can measure breathing patterns to enable the vehicle to react if a driver is stressed or relaxed.[72]

In addition to biometric information, sensors also collect behavioral information such as steering movements, time behind the wheel, and which dashboard instruments have been used.[73] Several Lexus car models, for example, assist drivers with parking and notify drivers if another car is in the next lane.[74] Automakers collect and retain this sensor data, but it is unclear how it is used other than for vehicle improvements.[75] It potentially could be sold to third-party marketers, used by insurance companies, or even used by employers or creditors to assess risk.[76]

Lastly, dedicated short-range communications ("DSRC") establish networks between vehicles and surrounding "intelligent" infrastructure.[77] These communications allow the connected car to

68. *See id.* at 122 (explaining that "sensor data will fuse to reveal more and different things about individuals' behaviors, habits, and future intentions.").

69. *See id.*

70. FUTURE OF PRIVACY FORUM, *supra* note 2, at 8.

71. *Id.*

72. *Id.*

73. *See, e.g.*, *Innovations*, BMW, http://www.bmwusa.com/standard/content/innovations/default.aspx (last visited Sept. 21, 2015) (explaining adaptive LED headlights, dynamic brake control, and surround view camera system). Mercedes-Benz's Attention Assist detects and initiates warnings when a driver is drowsy by sensing steering movements, driving time, and external influences like side-wind and uneven road surfaces. *Attention Assist*, MERCEDES-BENZ, http://www.mbusa.com/mercedes/benz/safety#module-3 (last visited Sept. 20, 2015).

74. *Lexus RX Safety*, LEXUS, http://www.lexus.com/models/RX/safety (last visited Sept. 21, 2015); Innovations, *supra* note 73.

75. Peppet, *supra* note 5, at 145.

76. Peppet, *supra* note 5, at 92.

77. FUTURE OF PRIVACY FORUM, *supra* note 2, at 10; *see also Vehicle-to-Infrastructure (V2I)*

sense, connect, and interact with the outside world.[78] With a constant broadcast and reception, connected cars respond to the surrounding environment: sensing the position, speed, and direction of nearby vehicles and hazards,[79] and issuing warnings directly to drivers.[80]

While these vehicle-to-vehicle and vehicle-to-infrastructure communications remain anonymous, without any specific location data individually identified,[81] it is unclear who can access and share this information, leaving many privacy concerns unanswered.[82] Furthermore, the collection of this data is problematic because there is no "OFF" switch.[83] Thus, a driver "will be deprived of basic choices about sending out data, which reflects the driver's behavior as much as it reflects that of the vehicle. That lack of choice and control deprives users of autonomy privacy."[84]

5. Big Data Technology in the Connected Car

"Big data" refers to the ways in which organizations and businesses "combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising benefits."[85] The data collected by the connected car is repackaged in the big data marketplace to produce

---

Communications for Safety, INTELLIGENT TRANS. SYS. JOINT PROGRAM OFFICE, U.S. DEP'T OF TRANSP., http://www.its.dot.gov/research_archives/safety/v2i_comm_safety.htm (last visited Oct. 2, 2015) ("Vehicle-to-Infrastructure (V2I) Communications for Safety is the wireless exchange of critical safety and operational data between vehicles and roadway infrastructure, intended primarily to avoid motor vehicle crashes."). Intelligent infrastructure in this Article refers to the infrastructure connected to vehicles, such as stoplights, lane markers, and buildings.

78. FUTURE OF PRIVACY FORUM, *supra* note 2, at 10; *see also* Glancy II, *supra* note 8, at 1631–32 (explaining that the DSRC unit collects and transmits information about a vehicle's location, speed, and direction of travel in the form of a Basic Safety Message to nearby vehicles, infrastructure, pedestrians, or bicyclists.).

79. FUTURE OF PRIVACY FORUM, *supra* note 2, at 10.

80. *Id.*; *see also* Glancy II, *supra* note 8, at 1633 ("The purpose of V2V safety data communications is to provide warnings to drivers, such as a stopped vehicle ahead, as well as to trigger automated systems, such as automated braking or lane alignment, to avoid a crash.").

81. Glancy II, *supra* note 8, at 1643.

82. FUTURE OF PRIVACY FORUM, *supra* note 2, at 11–12; FIPA Report, *supra* note 30, at 88 ("[F]urther privacy research is needed, with input from external security and privacy experts in order to properly assess the privacy risks inherent in the V2V system that is ultimately adopted…it remains to be seen how individual privacy is affected by future V2V and other ITS systems.").

83. Glancy II, *supra* note 8, at 1657.

84. *Id.*

85. Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA COMPUTER & HIGH TECH. L.J. 483, 484 n.1 (2014) (citing Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74 (2013)).

valuable insights into individuals' lives. Big data technology operates on "vastly larger amounts of data [than past data analytics technology], can tap data from any number of sources . . . and can do so in real time, as the data is produced or recorded."[86] Currently, the connected car uses big data technology to deliver real-time traffic and weather information[87] and to process the massive amount of data collected by the connected car. The benefits of big data may justify collecting vast amounts of data in some circumstances,[88] however, there are great opportunities for abuse, as automakers and third parties use big data in conjunction with cloud computing to "personalize services based on individual user profile[s] and categorize customers for target marketing purposes."[89]

In-car advertising is one way car manufacturers and third-party marketers may take advantage of driver data through big data technology. Automakers and companies in the vehicle technology industry have already patented technologies related to in-car advertising.[90] These companies can create advertising profiles using data collected on past travels and linking this data to similar profiles derived from internet usage and other consumer data.[91] Advertising could then be tailored specifically to the driver and channeled into the vehicle.[92] In addition, analyzing driving and purchasing habits to

86. FIPA Report, *supra* note 30, at 12.

87. *Id.*

88. *Id.* ("[T]he benefits of Big Data have become 'a justification for amassing vast amounts of information, processing the information for multiple and often unforeseen reasons beyond what the individuals who may have shared that information intended it for, and using that information to glean intelligence about individuals, groups, and even whole societies.'").

89. *Id.* at 28–29.

90. Kohler & Colbert-Taylor, *supra* note 30, at 122. Ford has patented in-car advertising technology and Ford, BMW, and Pandora are planning to release in-car advertising apps. *See id.* at 121 n.136; Tyler Wells Lynch, *CES 2014: Pandora Launches In-Car Advertising Platform*, USA TODAY (Jan. 6, 2014, 5:59 PM), http://www.usatoday.com/story/money/cars/2014/01/06/reviewed-ces-pandora-car-ads/4342261/; *see* Damon Lavrinc, *You Can Order a Pizza with Ford's New In-Car App*, WIRED (Jan. 7, 2014), http://www.wired.com/2014/01/ford-applink-dominos-parking.

91. Kohler & Colbert-Taylor, *supra* note 30, at 122.

92. *Id.* Ford's SYNC AppLink, for example, is compatible with the security company's ADT Pulse mobile app, enabling ADT customers to monitor their homes or businesses inside their cars, opening their door and adjusting lighting and temperatures through voice commands. This technology also raises significant security concerns in the event of a breach, possibly giving hackers access and control over the home. Lavrinc, *supra* note 90. SYNC AppLink also has a Domino's application, allowing drivers to order pizza through voice commands. The "Pizza Profile" stores frequent pizza orders and payment information, raising further security concerns in case of a breach. *Id.* Drivers might be more likely to order Domino's over another pizza company solely due to convenience and lack of options, a demonstration of how consumer choice is slowly disappearing.

determine likely impulse purchases could result in planned routes that lead a driver past a particular place of business without his knowledge.[93]

Big data uses data mining techniques and combines datasets to extract "both hidden information and surprising benefits."[94] Driver data generated by the connected car, when pieced together with data collected by websites and other connected devices, generates profiles of individuals' habits and behaviors, possibly revealing thoughts, ideas, and innovations.[95] Individuals' data is then used in a commercial context to create marketing profiles, sell advertisements, and conduct product analyses.[96] Because of the growing number of connected devices, the amount of data transmitted by consumers is increasing, leading companies to "monetize data collection for purposes extending far beyond the service provided."[97] Much of the type of data utilized by big data technology is not covered by California's current privacy laws, leaving this data unprotected, and drivers unaware of how their information is used.[98]

B. The Connected Car Legal Landscape in California

The following subsections discuss two major California privacy protection laws: COPPA and Shine the Light. These laws apply to any company that does business with a California consumer while operating a website.[99] Since many businesses across the country likely do business with at least one California consumer, [100] COPPA and Shine the Light impact the entire nation's privacy law framework.[101]

1. California Online Privacy Protection Act

COPPA requires website operators that collect California

93. *Id.* at 123; *see* Eloise Gratton, *If Personal Information is Privacy's Gatekeeper, Then Risk of Harm is the Key*, 24 ALB. L.J. SCI. & TECH. 105 at 189 (2014) (discussing how the individual would be frustrated by a sense of helplessness and powerlessness, affecting the social structure by "altering the kinds of relationships people have with the institutions that make important decisions about their lives.").

94. Bagley & Brown, *supra* note 85, 484.

95. *Id.* at 519.

96. *Id.* at 489.

97. *Id.* at 518.

98. Peppet, *supra* note 5, at 147–48.

99. Evans, *supra* note 20, at 205.

100. CAL. DEP'T OF JUSTICE, *supra* note 19, at i.

101. Evans, *supra* note 20, at 205.

residents' personal information to "conspicuously post"[102] a privacy policy and comply with it.[103] "Conspicuously post" means the privacy policy should either be on the business website's homepage or found through a distinguishable link on the homepage.[104] The privacy policy must identify the "personally identifiable information" collected and the categories of third parties with whom the operator shares that data.[105] The statute defines "personally identifiable information" as first and last name, address, e-mail address, telephone number, social security number, and any other identifier that permits the physical or online contacting of an individual.[106] COPPA also mandates that businesses disclose their response to "do not track" signals or other mechanisms that allow consumers to exercise choice over whether their personally identifiable information is collected online.[107] By enacting COPPA, the California Legislature intended to improve consumer knowledge as to whether personally identifiable information obtained by a website may be disclosed, sold, or shared.[108]

2. Shine the Light

Shine the Light requires businesses with California customers who collect personal information to provide either (1) a list of categories of personal information disclosed to other companies for marketing purposes during the preceding calendar year, or; (2) a privacy statement giving the customer a cost-free opportunity to opt out of such information sharing.[109] A business must comply with these notice requirements unless its privacy policy commits to obtaining opt-in consent before disclosing a customer's personal information to third parties or allows customers to opt out of such disclosures.[110] This

102. CAL. BUS. & PROF. CODE § 22577(b)(1)–(5) (Deering 2015).

103. *Id.* §§ 22575–579.

104. *Id.* § 22577(b)(1)–(5). Conspicuously post includes "posting the privacy policy through any of the following: (1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site." (2) An icon that is located on the homepage containing the word "privacy" in a color that is distinguishable linking to a web page where the privacy policy is posted. (3) A text link on the homepage including the word "privacy," written in capital letters in larger type or contrasting color that hyperlinks to a web page where the privacy policy is posted. (4) Any other functional hyperlink that would be noticeable by a reasonable person.

105. BUS. & PROF. § 22575(b)(1).

106. *Id.* § 22577(a)(1)–(6).

107. *Id.* § 22575(b)(5).

108. *Id.* Div. 8, Ch. 22 n.

109. CAL. CIV. CODE §1798.83(a) (Deering 2015).

110. *Id.* § 1798.83(c)(2).

law intends to give Californians the ability to understand with whom their information is shared and how it is used.[111]

Shine the Light only applies to personal information shared for direct marketing purposes, limited to soliciting the direct sale or leasing of goods by telephone, mail, or e-mail.[112] Personal information that must be disclosed includes name, age, address, e-mail, medical condition, property purchased, social security number, payment information, and credit history.[113] Although this law expands the definition of personal information beyond COPPA to include medical information and credit history, the meaning of "personal information" excludes much of the information collected by the connected car.

III. ANALYSIS

The evolution of big data contributes to the problem of privacy within the connected car. Big data technology threatens to undo de-identification mechanisms designed to separate personal information from non-personal information,[114] ultimately enabling re-identification.[115] Data collected by the connected car is particularly difficult to protect from re-identification because it "capture[s] such a rich picture of an individual, with so many related activities, that each individual in a sensor-based dataset is reasonably unique."[116] The assumption that anonymization can protect individuals' data is no longer true with the utilization of big data technology.[117] Both COPPA and Shine the Light rely on protecting information that is personally identifiable—leaving de-identified data unprotected.

The connected car collects data far beyond the types included in

111. ACLU, LOSING THE SPOTLIGHT: A STUDY OF CALIFORNIA'S SHINE THE LIGHT LAW 1 (2013), https://www.aclunc.org/sites/default/files/Losing%20the%20Spotlight%20-%20A%20Study%20of%20California%27s%20Shine%20the%20Light%20Law%20final.pdf.

112. CIV. § 1798.83(e)(2).

113. *Id.* § 1798.83(e)(7)(A)–(AA). Personal information includes the following: name and address; e-mail address; age or date of birth; names of children; e-mail or other addresses of children; number of children; age or gender of children; height; weight; race; religion; occupation; telephone number; education; political party affiliation; medical condition; drugs, therapies, or medical products or equipment used; the kind of product the customers purchased, leased, or rented; the kind of service provided; social security number; bank account number; credit card number; debit card number; bank or investment account, debit card, or credit card balance; payment history; information pertaining to creditworthiness, assets, income, or liabilities.

114. FIPA Report, *supra* note 30, at 12.

115. *Id.*

116. Peppet, *supra* note 5, at 130.

117. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706–07 (2010).

the definitions of personal information. Because personal information is the only type of data protected within California's privacy laws, drivers are left defenseless against companies collecting data that, when combined with other data, reveals intimate details about their lives.[118] Consumer control over data collected by the connected car is eliminated because automakers and third parties who collect data have unlimited power to gather and use data not falling within the definition of personal information.[119] COPPA and Shine the Light are the most applicable laws to the connected car's privacy issues because both broadly apply to all businesses, but neither law sufficiently addresses the unique privacy risks inherent in driver data.[120]

A. COPPA's Inadequacies

The connected car requires compliance with COPPA because automakers operate a commercial website and "online service."[121] Accordingly, they must disclose the types of personally identifiable information collected and the categories of third parties with whom they share that information. The privacy policy requirements in COPPA, however, have not been updated since 2008: long before connected cars became popular.[122] Vehicle manufacturers are using COPPA's baseline requirements that were created for traditional web

118. Bagley & Brown, *supra* note 85, at 520.

119. *Id.*

120. California Vehicle Code section 9951 addresses the data collected by EDRs. CAL. VEH. CODE § 9951 (Deering 2015). This section requires manufacturers to disclose EDRs in vehicle manuals and limits the use of this data to (1) the registered owner, (2) in response to a court order, (3) for the purpose of improving motor vehicle safety, and (4) a licensed motor vehicle dealer or automotive technician. Persons authorized to access this data may only share it among motor vehicle safety and medical research communities to advance safety, without disclosing the identity of the owner. While this law limits the accessibility of this data, it is silent regarding automobile insurance companies requiring the insured to grant access to EDR data in order to settle a claim or adjust rates. Peppet, *supra* note 5, at 92 ("Four states currently forbid insurance companies from requiring that an insured consent to future disclosure of EDR data or from requiring access to EDR data as a condition of settling an insurance claim. One state – Virginia – also forbids an insurer from adjusting rates solely based on an insured's refusal to provide EDR data."). *See, e.g.*, ARK. CODE ANN. § 23-112-107(e)(3)–(4) (2015); N.D. CENT. CODE § 51-07-28(6) (2015); OR. REV. STAT. § 105.932 (2015); VA. CODE ANN. § 38.2-2212(C.1)(s) (2015). Furthermore, the limited use requirement "for the purpose of improving motor vehicle safety" is not much of a limitation and is overly broad, since there are no requirements for what constitutes as "for the purpose of improving motor vehicle safety." Although this law is a start to protecting this type of information, implementing changes to COPPA and Shine the Light would more adequately protect data collected from EDRs.

121. Peppet, *supra* note 5, at 147; CAL. BUS. & PROF. CODE § 22575.

122. Peppet, *supra* note 5, at 148.

browsing on a computer, rather than applying the concepts to the connected car's unique characteristics.[123]

1. Personally Identifiable Information Under COPPA

Under COPPA, the term "personally identifiable information" refers to individually identifiable information about a consumer collected online and maintained by the website operator.[124] This definition excludes much of the information collected by the connected car, like location, accelerometer, data communicated via V2V or V2I pathways, and infotainment system data.[125] However, with the volume of data collected through the many ways individuals use the internet, big data analytics connect pieces of data together, possibly triggering a situation where "a single, insignificant piece of information may end up identifying an individual."[126] The Federal Trade Commission recognizes that the distinction between personally identifiable information and non-personally identifiable information is rapidly losing significance due to technological innovations, but California's lagging law leaves manufacturers compliant with a limited definition of personal information under COPPA.[127]

a. COPPA excludes behavioral & sensor data

Behavioral and sensor data collected by the connected car, such as braking patterns, seat positions, and biometric data, do not fall within COPPA's definition of personally identifiable information. This behavioral and sensor data is extremely valuable and can indicate personal habits and characteristics, such as occupant size from seat position or eating habits from their "Pizza Profile," built from the Ford

123. Peppet, *supra* note 5, at 147; *see also id.* at 144 (After describing a variety of Internet of Things privacy policies, concluding that these policies are often unclear about whether sensor data counts as personal information, and most privacy policies allow manufacturers of these devices to sell and share non-personal information in an unrestricted manner.).

124. BUS. & PROF. § 22577(a).

125. *Id.* § 22577(a)(1)–(7) (including only name, address, e-mail, telephone number, social security number, an identifier permitting the physical or online contacting of a specific individual, and information collected online maintained in personally identifiable form in combination with one of the listed above).

126. Gratton, *supra* note 93, at 120–21.

127. FEDERAL TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 19 (2012) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter FTC 2012 Recommendations] ("The traditional distinction between PII and non-PII has blurred and that it is appropriate to more comprehensively examine data to determine the data's privacy implications.").

Domino's application. Potential harm arises when those with access to this data are able to utilize it to conduct risk assessments in the insurance, employment, credit, or financial context.[128] Automakers and third parties could also take advantage of this data by linking it to much larger data sets to form a complete consumer profile used to predict and guide purchases and decisions, possibly in discriminatory ways.[129]

b. COPPA does not protect location data

One of the most significant types of information excluded from COPPA's definition of personal information is location data.[130] Senator Mark Leno of California proposed to add location information to COPPA.[131] This addition would mandate operators of mobile applications to provide clear and conspicuous notice upon installation of the app of when, how, and why consumer location information will be collected, used, and shared.[132] This bill would also require mobile application operators to obtain a user's affirmative consent before collecting location data, as well as requiring operators to separately obtain consent before disclosing such information.[133] This bill empowers users to have control over their location data and opt-in or refuse to share with third parties.

Although this bill marks another form of California leadership within the privacy space, the bill leaves open the question of location data collected by the connected car. It is unclear whether "mobile application" covers the applications within infotainment systems. Even if the applications connected to a driver's cell phone obtained user consent on the application within the phone, the driver likely remains unaware that his or her use of the application through the car will also grant application operators and third parties the permission to collect and use the location data derived from the vehicle.[134]

128. Gratton, *supra* note 93, at 190; Peppet, *supra* note 5, at 126–27.

129. Gratton, *supra* note 93, at 123. Amazon, for example, was accused of adaptive pricing using cookies that would raise the price of certain items in accordance with the profile of the potential purchaser.

130. BUS. & PROF. § 22577(a).

131. S.B. 576, 16 Reg. Sess. (Cal. 2015). After not receiving enough votes in early 2015, this bill will likely be introduced again in 2016.

132. *Id.*

133. *Id.*

134. *See* Bagley & Brown, *supra* note 85, at 494 (explaining lack of consumer awareness of the cumulative effects of "plugging into one brand's ecosystem for their online experience," giving

Furthermore, it is easy to imagine the difficulty in closing applications while driving, leaving many applications collecting location information while the application is not being used at that moment. These mandates need to be adapted for the connected car by, for example, requiring companies to obtain consent through voice activation or visually displayed notice and consent notifications on the vehicle's display. Although Senator Leno's bill might cover location data collected through infotainment applications connected to a driver's mobile phone, the bill leaves out location data collected by OBDs, EDRs, and V2V or V2I technology.

Location data exposes the exact vehicle location at any given time and can "reveal intimate details of a person's private life, such as the fact that she is . . . interviewing for a job with a competitor, participating in a protest, or visiting a medical clinic."[135] The sensitivity of this type of data should be reflected in COPPA's definition of personal information because it can be used to embarrass, draw discriminating inferences, or create marketing profiles used in unexpected ways.[136]

2. "Conspicuously Post" Is Not Adapted to the Connected Car

COPPA mandates disclosure by requiring website operators to "conspicuously" post a privacy policy.[137] "Conspicuously post," however, is not adapted to any other device besides a traditional webpage on the computer.[138] Disclosure of connected car data is limited to the privacy policies on the automaker's website, not readily available to the driver while using the services while inside the vehicle.[139]

Ford SYNC's privacy policy, for example, is split into two, both accessible from the Ford main website: the Ford Privacy Policy and

broad consent to "an array of unanticipated information disclosure, sharing, and aggregating among third parties").

135. FIPA Report, *supra* note 30, at 63.

136. *Id.*

137. BUS. & PROF. § 22575(a).

138. *Id.* § 22577(b)(1)–(5). The statute's definition of "conspicuously post" is satisfied if the website operator posts the privacy policy on the first significant web page visited or homepage, through a hyperlink on the homepage including the word "privacy" and in a different font color or size, or through "any other reasonably accessible means of making the privacy policy available for consumers." This last method of satisfaction is extremely broad.

139. *Lexusenformappsuite.com Privacy Policy*, LEXUS (2015), https://www.lexusenformappsuite.com/privacyPolicy; *SYNC Terms and Conditions*, FORD (2015), https://owner.ford.com/tools/account/sync-terms-and-conditions.html.

the SYNC Terms and Conditions.[140] The Privacy Policy contains Ford's response to opt-out or "do not track" mechanisms, the methods of collection, and reasons for collection,[141] while the SYNC Terms and Conditions describe the types of information collected, used, and disclosed specifically by the SYNC infotainment system.[142] Although complying with COPPA, Ford's privacy policies grant Ford the ability to collect and use a broad range of data recorded without the express affirmative consent of the user, regardless of whether the user has read the policies.[143] Although Ford's policies state that Ford will not share personal information with independent third parties, Ford has broad range to share this data with parties who contribute to the SYNC services.[144] These service providers would include companies operating applications such as Domino's or ADT. With this growing list of service providers, consumers are unknowingly giving up control over their personal information.[145] Ford also reserves the right to "use and share any aggregate (non-personally identifiable) information it obtains . . . for any purpose."[146] Interpreting this provision, most of the data collected by SYNC services is not personally identifiable and therefore can be freely used and shared with anybody, even parties not affiliated with Ford SYNC whatsoever.

Ford SYNC is just one example of an automaker's ability to collect, use, and share driver data. This data can easily be monetized for analyzing purchasing habits and preference insights, while also revealing a user's risk-taking behavior, daily routines, health developments, and reputation-harming activities.[147] To enable drivers to learn how their information is being used, the definition of

140. *Ford.com Privacy Policy*, FORD, http://www.ford.com/help/privacy/ (last visited Oct. 20, 2015); *SYNC Terms and Conditions*, *supra* note 139.

141. *Ford.com Privacy Policy*, *supra* note 140.

142. *SYNC Terms and Conditions*, *supra* note 139.

143. *Id.* The Terms and Conditions state that Ford may collect, log, store, and share with Ford and other SYNC service providers data including cell phone number, travel information, address information used for direction requests, and "other information you have provided," such as business directory look-ups, and sports and news favorites.

144. *SYNC Terms and Conditions*, *supra* note 139.

145. *See* Bagley & Brown, *supra* note 85, at 494 (There is lack of consumer awareness of the cumulative effects of sharing data with one "ecosystem," giving broad consent to "an array of unanticipated information disclosure, sharing, and aggregating among third parties.").

146. *SYNC Terms and Conditions*, *supra* note 139.

147. Kohler & Colbert-Taylor, *supra* note 30, at 127; Bagley & Brown, *supra* note 85, at 518–19; *see also* FIPA Report, *supra* note 30, at 65 (giving the example of "a single trip to a gynecologist's office tells little about a woman, but a trip followed a few weeks later by a visit to a baby supply store tells a different story.").

personally identifiable information should be expanded to include sensor data, data generated by OBDs, location information, biometric data, and data generated by infotainment systems.

B. Consent & Shine the Light

California's Shine the Light law aims to touch on a separate issue not addressed by COPPA: the ability to opt out. Shine the Light requires businesses who collect and disclose personal information for direct marketing purposes to provide a list of categories of personal information, along with a list of companies to whom it was disclosed upon request.[148]

Shine the Light has several exemptions. First, companies are exempt from providing customers with such information if their privacy policy gives the customer a cost-free opportunity to opt out of information-sharing or makes clear that the company only shares personal information upon obtaining affirmative consent.[149] Shine the Light also only applies to companies sharing of personal information for direct marketing purposes.[150] The definition of "direct marketing purposes" is limited to the solicitation of a lease or sale of goods or services through mail, telephone, or e-mail.[151] Lastly, Shine the Light provides an exemption for disclosures to third-party joint service providers provided that these third parties do not disclose the information other than to carry out the joint service.[152] Although the legislature passed Shine the Light to inform consumers about who uses their personal data, the law has many inadequacies preventing drivers from understanding how their information is collected and used by the connected car.[153]

1. "Personal Information" Is Too Narrow

Shine the Light's definition of personal information only includes information that, when it was disclosed, identified, described, or was able to be associated with an individual.[154] Much of the information collected by the connected car does not fall within the categories of

148. CAL. CIV. CODE § 1798.83(a) (Deering 2015).
149. *Id.* § 1798.83(c)(2).
150. *Id.* § 1798.83(a).
151. *Id.* § 1798.83(e)(2).
152. *Id.* § 1798.83(d)(1)(E).
153. ACLU, *supra* note 111, at 9.
154. CIV. § 1798.83(e)(7).

personal information listed in Shine the Light. For example, the definition excludes location data, data regarding driving behavior, and data collected by infotainment systems showing user preferences and habits. The list of what information is considered personal information is broader in Shine the Light than COPPA, as it includes height, weight, medical condition, education, and political party affiliation. However, the requirement that this information can be identified when it was disclosed narrows the law's application dramatically. All of this data can be linked back to the individual through big data analytics technology after disclosure.[155] Drivers have no means to learn how companies share data falling outside the definition of personal information, even if it is identifiable after disclosure. Because of the narrow definition of personal information in Shine the Light, most connected car data can be freely disclosed to third parties without the knowledge of drivers.

2. "Direct Marketing Purposes" Leaves Data Unprotected

Shine the Light requires compliance only from those businesses that disclose personal information for "direct marketing purposes."[156] Direct marketing purposes is limited to the direct sale or leasing of goods or services through postal mail, telephone, or email.[157] The problem with this limitation arises because this definition excludes purposes other than a solicitation for a sale or lease of goods through methods other than mail, telephone, or email. Limiting this law to apply only when information is disclosed for the direct sale or lease of goods or services leaves out any information used for other purposes such as risk assessment (for insurance, credit, or employment purposes) or soliciting a consumer to simply use a product or service rather than soliciting a consumer to purchase a product or service.[158] The second part of this definition limits the application of Shine the Light to direct marketing purposes through postal mail, telephone, or email.[159] This excludes direct marketing such as banner ads, pop-up

155. Bagley & Brown, *supra* note 85, at 489–90; *see also* Ohm, *supra* note 117, at 1704.

156. CIV. §1798.83(a).

157. *Id.* §1798.83(e)(2).

158. Examples of a product or service that cannot be purchased include Facebook, Twitter, Instagram, other social media sites, online marketplaces such as Amazon, Ebay, and Craigslist, and music streaming services such as Spotify or Pandora. These businesses may solicit customers to use their website rather than a competitor's website without soliciting customers to purchase a specific product.

159. CIV. § 1798.83(e)(2).

ads, personalized recommendations, and other forms of digital advertising.

The narrow application of this portion of Shine the Light excludes many of the disclosures made in connection with information collected by the connected car. Automakers and third parties would be exempt from complying with the law for disclosures of personal information made for non-direct marketing purposes. For example, the connected car collects data that could pertain to an individual's risk-taking behavior, such as how quickly the driver accelerates or breaks or whether they change the radio or talk on the phone while driving.[160] If this data is shared with a third party, such as an insurance company, for the purpose of risk assessment rather than to solicit a sale, the business would not be required to comply with Shine the Light and the driver would be left in the dark regarding how their information is being used in a potentially discriminatory way.[161] Similarly, infotainment systems collect a wide variety of information regarding user preferences, which can be "highly revealing of an individual's personal life, values, [and] interests . . . and is obviously sensitive given how it can be used to profile, target, and discriminate among individuals in unacceptable ways."[162] Under Shine the Light, this information, despite its sensitive nature, could be disclosed in compliance with the law, if disclosed for purposes other than to solicit a sale.

3. Shine the Light's Exemption for Disclosures to Joint Service Providers

Automakers are exempt from complying with Shine the Light's disclosure requirements for disclosures to third-party joint service providers, provided that these third parties do not disclose customers' personal information for purposes other than to carry out the joint service.[163] The problem with this exemption is that drivers are not likely to expect that their information may be disclosed to all of the third parties involved in providing the features of the connected car.[164]

160. FIPA Report, *supra* note 30, at 61.

161. *Id.* at 72; Peppet, *supra* note 5, at 126–27.

162. FIPA Report, *supra* note 30, at 64.

163. CIV. § 1798.83(d)(1)(E).

164. ED MARKEY, TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 11, (2015) http://www.markey.senate.gov/imo/media/doc/2015-02-06_Markey Report-Tracking_Hacking_CarSecurity%202.pdf.

The web of third parties involved quickly grows and makes it difficult for consumers to track who has access to their data. Automakers do not make an effort to educate drivers about all of the third parties involved in providing connected car features, nor are they mandated to do so due to this exemption.[165] Although the exemption requires these third parties to keep the information confidential, that requirement leaves open the ability to use the information to carry out the joint service, which may include disclosures to additional parties who are necessary to provide the service.

The connected car's infotainment system and other features rely on partnerships with third parties to carry out the service. For example, many infotainment systems include third party applications such as Pandora or a news application.[166] Furthermore, data collected by the connected car is shared with many players, including service providers, affiliated dealers and financing companies, mobile network operators, and smartphone operating system providers.[167] The connected car's features are rapidly expanding, and much of that expansion is dependent on the various companies that are evolving to join the connected car world. This rapid expansion increases the types of data disclosures that are exempted from Shine the Light's requirements, leaving consumers increasingly unprotected.

4. Shine the Light's Opt-Out Exemption

Shine the Light also provides an exemption for businesses whose privacy policy allows customers to opt out of data disclosures or whose policy is to only disclose information upon obtaining affirmative consent.[168] Businesses who have the opt-out mechanism or consent requirement do not need to share which types of personal information is disclosed, nor to whom it is disclosed. If a business provides such an opt-out mechanism, the consumer is not entitled to learn what information the business has already shared prior to opting out.

Opt-out mechanisms are not adequately applied to the connected car. Drivers must go to the automaker's website to find a privacy

165. *Id.* at 11.

166. FUTURE OF PRIVACY FORUM, *supra* note 2, at 8–9; *see also Lexus Enform: App Suite*, *supra* note 7 (showing the variety of applications accessible within Lexus vehicles).

167. FIPA Report, *supra* note 30, at 73.

168. CIV. § 1798.83(c)(2).

policy that may or may not contain opt-out instructions applicable to the connected car. Lexus, for instance, is exempt from complying with Shine the Light's disclosure requirements because the company provides customers an opportunity to opt out.[169] The opt-out mechanism links customers to the Digital Advertising Alliance Consumer Choice Page, which customers can only use to opt out if their browser does not block third-party cookies.[170] This method of opt-out is only functional on a browser, leaving no way to opt out of disclosure of data collected by the connected car. Unlike a website displayed on a computer, much of connected car data is collected by instruments without a screen. Even those that do have a screen, like the infotainment system, do not display the privacy policy or opt-out instructions on that screen.

Furthermore, many automakers decline to provide an opt-out mechanism, requiring drivers to discontinue using certain features if they do not want their data to be collected and shared.[171] Ford SYNC's Privacy Policy, for example, states "[i]f you don't consent or wish to disclose this information, do not activate or use SYNC Services."[172]

IV. PROPOSED SOLUTIONS

A. Broaden COPPA to Create Notice of Data Collected by the Connected Car

COPPA's limited definition of "personally identifiable information" leaves driver data unprotected. Furthermore, COPPA's requirement that companies "conspicuously" post privacy policies is not adapted to the unique features of the connected car.

1. Expand the Definition of Personally Identifiable Information

Because nearly all automakers maintain a website, they must comply with COPPA. Under COPPA, website operators (in this case, automakers) must disclose the types of personally identifiable information collected and the categories of third parties with whom

169. *Lexus Online Privacy Statement, Advertising/Behavioral Targeting: How To Opt-Out*, LEXUS, http://www.lexus.com/privacy/online-statement#choice-and-access (last visited Nov. 1, 2015).

170. DIGITAL ADVERTISING ALLIANCE CONSUMER CHOICE PAGE, http://www.aboutads.info/choices/ (last visited Nov. 1, 2015).

171. *See SYNC Terms and Conditions*, *supra* note 139.

172. *Id.*

that information is shared.[173] However, much of the data collected by automakers and third-parties involved in the connected car is excluded from COPPA's disclosure requirements because it falls outside the definition of personally identifiable information.[174] Therefore, consumers have no way to know whether automakers collect or disclose information falling outside the definition of personally identifiable information, even if that information is highly revealing of an individual's habits and behaviors. Expanding COPPA's definition of personally identifiable information to include the sensor and behavioral information collected by the connected car will increase drivers' awareness of how their information is being used.

COPPA's definition of personally identifiable information should include information collected by OBDs, infotainment systems, and internal car sensors. OBDs collect a breadth of information, such as location data, driving times, mileage, frequent sudden braking or accelerating, overall engine health, and other driving behavior data.[175] This data is stored over time and is readily accessible by automakers and authorized third parties,[176] making it easy for those with access to draw conclusions about a driver's daily patterns and behaviors.[177] Furthermore, this data can also be used for purposes of risk assessment in the insurance context, possibly discriminating against a driver without his or her knowledge.[178]

Information collected by infotainment systems poses similar privacy risks to information collected by OBDs, and should be classified as personally identifiable information. While some information collected by infotainment systems is already personally identifiable under COPPA's definition,[179] these systems collect much more information that falls outside the definition.[180] They collect and

173. CAL. BUS. & PROF. CODE § 22575(b)(1) (Deering 2015).

174. *Id.* § 22577(a).

175. FIPA Report, *supra* note 30, at 22–24.

176. *Id.* at 24.

177. Peppet, *supra* note 5, at 122; *see also* Kohler & Colbert-Taylor, *supra* note 30, at 126–27 ("In the realm of non-autonomous but highly connected vehicles, such data would include information about a user's driving habits, such as information about rates of acceleration, speed, braking data, and the like, which could be used to demonstrate liability in case of accidents, to form an individualized and empirical basis for car insurance rates").

178. Peppet, *supra* note 5, at 118.

179. *Id.* Examples of information collected by infotainment systems that already falls within the definition of personally identifiable includes subscriber information, like e-mail, payment information, and phone numbers.

180. FUTURE OF PRIVACY FORUM, *supra* note 2, at 9–10; Glancy II, *supra* note 8, at 1658.

store information that is incredibly valuable to third-party marketers, advertisers, and service providers, such as frequented restaurants, location data, and the contacts stored in the driver's phone.[181] To understand how this information is used, drivers should have the opportunity to learn what information is collected and with whom it is shared.

Biometric data recorded by internal sensors within the connected car should also be classified as personally identifiable. This data includes pulse and body temperature measured by conductive sensors in the steering wheel, facial recognition data, and breathing patterns measured by the seatbelt.[182] This data is highly personal and those with access to it can make intimate inferences about a driver's physiological, psychological, behavioral, and health states.[183] Due to the sensitivity of biometric information, drivers should be able to understand exactly what information is collected, and the types of companies to which it is disclosed.

Lastly, location data, no matter how it is collected, should be classified as personally identifiable information. COPPA's current definition includes "any other identifier that permits the physical or online contacting of a specific individual."[184] However, since this data might not be disclosed in real-time, the past location data would not permit the physical contacting of a specific individual. Nonetheless, location data can be easily identifiable and can paint a picture of an individual's every move, leading to inferences about intimate details of a driver's private life.[185]

Senator Leno's proposed bill could address some of the privacy concerns regarding location data if it were expanded to include location data collected by the connected car. The bill seeks to mandate mobile application providers to provide notice of how consumer location information is collected, used, and shared.[186] This bill, however, only applies to location data collected through mobile applications. It should be expanded to include location data collected

181. FUTURE OF PRIVACY FORUM, *supra* note 2, at 9–10.

182. *Id.* at 8.

183. Peppet, *supra* note 5, at 122.

184. CAL. BUS. & PROF. CODE § 22577(a)(7) (Deering 2015).

185. Your car knows what time you leave in the morning, what route you take most often, where you drop your children off at school, where you frequently stop for lunch, and whether you have recently visited the doctor's office.

186. S.B. 576, 16 Reg. Sess. (Cal. 2015).

by the connected car.

Sensor data can be combined to draw intimate inferences about an individual's private life—inferences giving insight into levels of relaxation or stress, or more simply, a driver's daily routine.[187] Expanding the definition of personally identifiable information to include location data and data collected by OBDs, infotainment systems, and other internal sensors enables drivers to learn about the various ways their information is collected and used.

2. Adapt COPPA Privacy Policies to the Connected Car

COPPA's insufficient "conspicuously" post requirement[188] needs to be adapted to meet the unique privacy risks posed by the connected car. COPPA clearly applies to automakers and related third parties who operate features of the connected car because many of these features take advantage of the internet. To comply with COPPA, however, these businesses need only post privacy policies on their website,[189] a place many drivers would likely never think to look to find information relating to the data collected by their vehicle.

To provide drivers with notice of how their information is collected and used, automakers should be required to post privacy policies in places reasonably related to the car and easily accessible by drivers. Privacy policies should be available on the screen inside the vehicle, perhaps popping up when the driver turns on the car. Automakers should post a simplified notice that the vehicle collects, stores, and uses driver data on the corner of the windshield, similar to an oil change sticker. Additionally, privacy policies should be available when the car is purchased or leased in a separate, noticeable document. Automakers should also have distinct privacy policies posted on their websites, separate from their website policies. Lastly, privacy policies for connected car features should be easily found inside the owner's manual or in a separate guide to driver data privacy.

B. Consent Opportunities in Shine the Light

Shine the Light's limited definition of personal information and its variety of exemptions exclude much of the data collected by the connected car. Consumers have no way to learn how their sensitive

187. Peppet, *supra* note 5, at 121–22; FIPA Report, *supra* note 30, at 65.
188. BUS. & PROF. § 22575(a).
189. *Id.*

driver data is disclosed to third parties nor do consumers have a method of opting out of such disclosure. The reforms outlined below seek to increase the level of transparency between connected car manufacturers, service providers, and drivers.

1. Expand the Definition of Personal Information

The definition of personal information in Shine the Light should be expanded in the same way proposed above for COPPA, including data collected from OBDs, infotainment systems, and internal sensors. Location data should be included no matter how that data is collected. The definition should be consistent with other California privacy laws and include all information "reasonably linked" to a consumer.[190] Shine the Light provides awareness to consumers of which third parties businesses have disclosed their personal information to,[191] as opposed to COPPA which focuses on the categories of third parties with access to consumers' personal data.[192] By broadening the definition of personal information, Shine the Light would enable drivers to learn exactly which companies received their information.

2. Broaden the Application Beyond Direct Marketing

Currently, Shine the Light only applies to a business that "knows or reasonably should know that the third parties used the personal information for the third parties' direct marketing purposes."[193] "[D]irect marketing purposes" includes soliciting a sale or lease of goods or services through telephone, email, or postal mail.[194] This definition leaves out disclosures to businesses who use the personal information for other purposes, such as marketing services not intended to solicit a sale.[195] The definition also leaves out soliciting a sale or lease through alternative marketing channels, such as pop-up advertising, banner advertisements, and other forms of digital marketing not through email. This demonstrates how Shine the Light has not kept up with technology's evolution. To enable drivers to learn

190. CAL. CIV. CODE § 1798.80(e) (Deering 2015). COPPA has a separate definition of personally identifiable information.

191. *Id.* § 1798.83(a)(1).

192. BUS. & PROF. § 22575(b)(1).

193. CIV. § 1798.83(a).

194. *Id.* § 1798.83(e)(2).

195. For example, a service that a consumer uses but does not purchase is Facebook or LinkedIn.

how their data may be used to create detailed marketing profiles, "direct marketing purposes" should include any marketing or advertising, beyond solicitations to purchase a good or service, as well as apply to solicitations through other methods of communication and forms of digital marketing like pop-up and banner advertisements. Drivers will then be able to learn exactly who is using their information for any marketing purpose. Expanding the definition of direct marketing purposes to include all types of marketing and advertising will broaden the applicability of Shine the Light and allow for privacy protection to keep up with technological advancements.

3. Revise the Exemption for Third Party Joint Service Providers

Under Shine the Light, automakers are exempt from disclosing their sharing practices with third-party joint service providers.[196] Because of the increasing number of third-party partners involved with the connected car,[197] this exemption is overly broad. It may be necessary for automakers to partner with third parties to provide the maximum amount of features within the connected car, but these automakers should still be mandated to disclose the names of the third party partners. Ford, for example, partnered with Dominos to enable drivers to order pizza from within their car.[198] Ford also partnered with ADT to allow drivers to maintain their home security systems through the SYNC infotainment system.[199] Under the current Shine the Light law, Ford would not be required to disclose whether it shares personal information with Dominos and ADT because these companies offer a joint service. Shine the Light's purpose—to increase transparency—would be better served if the law required automakers and other businesses to disclose which third parties receive customer information, whether or not the third party is an official partner.

4. Apply Opt-Out Mechanisms to the Connected Car

Businesses that provide an opt-out option or only disclose data upon receiving affirmative consent are exempt from complying with

196. CIV. § 1798.83(d)(1)(E).

197. One example of the diverse array of third-party partners is Ford's partnership with Domino's and ADT. Lavrinc, *supra* note 90. Lexus is also increasing the number of third party partners, such as with applications for Pandora and OpenTable. *Lexus Enform: App Suite*, *supra* note 7.

198. Lavrinc, *supra* note 90.

199. *Id.*

Shine the Light's disclosure requirements,[200] yet these opt-out mechanisms are not practically applied to the connected car. First and foremost, for maximum protection, companies should be required to obtain affirmative consent in order to collect and disclose any data at all. Automakers could obtain affirmative consent through a separate and distinct consent form when the driver purchases or leases the vehicle. Additionally, consent could be obtained through clicking an "I agree" button at the bottom of the privacy policy on the car's display. After giving consent, however, a user should be able to opt out of all or certain methods of data collection and disclosure through a user-friendly interface.[201]

Currently, drivers are not able to obtain a list of third parties at all if the automaker provides an opt-out mechanism. To increase consumer awareness and control over their data, companies should be mandated to provide drivers with a list of third parties with whom the automaker has shared their information up until the point the driver decided to opt out.

Furthermore, the method of opting out should be tailored to the connected car. Automakers who provide an option to opt out may be limited to the data collected via the website, rather than the vehicle. Drivers, therefore, have no way to opt out of data collected by their car. An opt-out method should be readily accessible from within the car, perhaps on the vehicle's display or from a mobile phone. The automaker should have a separate opt-out page accessible through its website that is connected to the driver's car, making sure that the opt-out decision is transferred to the vehicle's collection of information.

V. CONCLUSION

Data collected by the connected car is often highly personal—revealing intimate insights into a driver's daily life, behavioral habits, and preferences. Third parties may use these insights for unexpected purposes such as advertising, building individual marketing profiles, and assessing risk. Although California is a leader in privacy within the United States, COPPA and Shine the Light's inadequacies threaten driver privacy because the types of information collected by the

200. CIV. § 1798.83(c)(2).

201. Brill, *supra* note 5, at 216 ("The user interface is also critical: it should be user-friendly, and industry should provide a one-stop shop so consumers can learn about the tools that all data brokers provide, and the choices consumers can make about the use of their data.").

connected car do not fall within the definitions of personal information, enabling automakers and third-parties to freely collect, retain, and disclose this data. Big data technology easily identifies connected car data to a specific driver, making the effect no different from the current definition of personal information.

COPPA and Shine the Light seek to protect privacy by increasing consumer awareness and control through notice and consent opportunities. By expanding the definition of personal information within COPPA and Shine the Light and broadening the application of both of these laws, drivers would be provided the opportunity to learn how the data collected by their vehicles is used. COPPA and Shine the Light's mandated notice and consent opportunities should be adapted to the connected car's unique characteristics, enabling drivers to maintain control over their data from inside their vehicles. Revising COPPA and Shine the Light to include data collected by the connected car is the first step toward paralleling drivers' level of privacy and control over their data with rapidly growing connected car technologies.