Regulating Data Privacy of Connected Vehicles: How Automotive Giants Can Protect Themselves and Their Golden Goose

Halie B. Peacher*

Abstract

The growth of automotive technology and data privacy are fundamentally intertwined. Auto manufacturers can collect 25 GB of data from vehicles at the rate of 2 GB per hour. At that rate, automotive manufacturers may increase profits, enhance driving experiences, and make driving safer. Companies that own and sell the data from these vehicles are expected to gain a thirty-five percent increase in revenue.

With this great monetary benefit, comes the decrease in consumer privacy and the increase in the exploitation of a consumer's everyday life. This exploitation ranges from a company's access to everything from text messages to driving history. Thus, as the rat race for profits speeds up and becomes more competitive, companies will have to maintain compliance with regulations such as the Global Data Protection Regulation ("GDPR") and the California Consumer Protection Act ("CCPA"). These regulations are put into place to stifle the exploitation of consumer data and to ensure the protection of consumers. Additionally, as companies gain more access to consumer data, companies will likely face great liability any time there is a data breach or a hack that leads to stolen consumer data.

This article looks at the history of automobiles, privacy laws, and data breaches, and explores how the future of automobiles is impacted by the increase in consumer data consumption. Specifically, this article analyzes: (1) how manufacturers can maintain compliance with the GDPR and the CCPA to protect all consumers who encounter a connected vehicle; and (2) whether the consumer or the automobile company is liable for a potential data breach.

INTRODUCTION

In 2018, "32 of 44 [automotive] brands" offered wireless data connection in their cars.[1] Connected cars collect about 25 GB of data per hour, and out of the 25 GB collected, 2 GB per hour are digitally transferrable to the manufacturer.[2] The ability to connect data to almost anything allows companies to increase their profits exponentially.[3]

Figuratively speaking, whoever owns the data also owns the golden goose.[4] The companies that own and sell the data from these vehicles are expected to gain a thirty percent increase in revenue.[5] The rat race for profits has begun and will be more competitive as companies find more ways to exploit consumer data for their monetary benefit.[6]

---

1 Jeff Plungis, *Who Owns the Data Your Car Collects?*, CONSUMER REPS. (May 2, 2018), https://www.consumerreports.org/automotive-technology/who-owns-the-data-your-car-collects/.

2 Jiri Chejn, *Time is Running Out . . . is Your Car GDPR Compliant?*, SQUIRE PATTON BOGGS (May 4, 2018), https://www.securityprivacybytes.com/2018/05/time-is-running-out-is-your-car-gdpr-compliant/.

3 *See* Peter Holley, *Big Brother on Wheels: Why Your Car Company May Know More About You Than Your Spouse*, WASH. POST (Jan. 15, 2018), https://www.washingtonpost.com/news/innov ations/wp/2018/01/15/big-brother-on-wheels-why-your-car-company-may-know-more-about-you-than-your-spouse/?noredirect=on&utm_term=.3ec94c927856 (explaining how car companies are incentivized to make a profit off of the data collected from vehicles); *see also* Bloom et al., *Self-Driving Cars and Data Collection: Privacy Perception of Networked Autonomous Vehicles*, 13 SYMPOSIUM ON USABLE PRIVACY AND SECURITY 357, 357 (July 12-14, 2017), https://www.usenix.org/system/files/conference/soups2017/soups2017-bloom.pdf (explaining how vehicles are capable of collecting an entire city's residents' location and movement data by storing and analyzing a vehicle's sensor data).

4 *See The Goose & the Golden Egg*, LIBR. OF CONGRESS, http://read.gov/aesop/091.html (explaining possessing the golden goose leads to riches from their golden eggs).

5 *See Automotive Revolution – Perspective Towards 2030*, MCKINSEY & CO. 1, 4 (Jan. 2016), https://www.mckinsey.com/~/media/mckinsey/industries/high%20tech/our%20insights/disruptive%20trends%20that%20will%20transform%20the%20auto%20industry/auto%202030%20report%20jan%202016.ashx (showing that shared mobility and connectivity sensors might expand automotive revenue by $1.5 trillion).

6 *See* Cherie Hu, *What Does Music Have to Gain from the Future of Transportation? More Than You Might Think*, FORBES (Nov. 6, 2018), https://www.forbes.com/sites/cheriehu/2018/11/06/music-future-transportation-ridesharing-5g-startups/#496449b97169

Part I of this comment explains the background of the automotive industry and data privacy. In addition, Part I explains the background of the Global Data Protection Regulation ("GDPR"),[7] the California Consumer Protection Act ("CCPA"),[8] and explains how consumers are impacted when there is a privacy or data breach. Part II analyzes: (1) whether and how automobile companies will comply with the international regulation, the GDPR, and the state regulation, the CCPA, to protect all consumers that will encounter a connected vehicle; and (2) whether the consumer or the automobile company is liable for a potential data breach.

In Part III of this comment, one recommendation will be made: how automotive companies may comply with regulations and create a legal policy that best protects both the consumers and the company. Finally, Part IV concludes by establishing how automotive companies may comply with such regulations.

I. Where Did Data Collection Begin and How Has it Evolved?

To visualize the exploitation of consumer data through automobiles, it is essential to understand what data companies may use and what regulations are in place to protect consumers. The section below will discuss: (A) automotive data privacy history; (B) connected vehicle technology; (C) international and national data privacy regulations; and (D) how consumers, bystanders, and automobile companies are impacted.

A. Automotive Data Privacy Overview

Vehicle data collection is not as novel as it may appear. Since the 1980s, automotive manufacturers have utilized some form of onboard diagnostic ("OBD-II") ports and event data recorders

(explaining how the music and automotive industries are teaming up to create a more "fleshed-out, personalized" experience).

7 Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

8 California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100-1798.198 (West 2018).

("EDRs").[9] The manufactures install the OBD-II[10] and EDR[11] systems to enhance vehicle safety and to better understand customer needs.[12]

Data is collected from any vehicle manufactured after 2014 allowing companies to access and track personal information.[13] This data is likely generated from one's infotainment system.[14] On its face, this appears to be a lot of information accessible by manufacturers, however, it is not even the beginning of what manufacturers will be able to access.[15]

Tesla, Waymo, and GM are automotive innovation leaders that access the most automobile data.[16] For example, Tesla's vehicles

---

9 *See* Plungis, *supra* note 1 (showing companies offered "built-in cellular data links for safety and concierge services").

10 *See* Stephen Edelstein, *From Dongles to Diagnostics, Here's All You Need to Know About OBD/OBD II*, DIG. TRENDS (Apr. 7, 2017), https://www.digitaltrends.com/cars/everything-you-need-to-know-about-obd-obdii/ (showing OBD-II provides the ability to conduct emission testing and to analyze and repair internal issues).

11 *See id.* (explaining the EDR is a device that records vehicle and occupant data to show what happened pre- and post-crash).

12 *See id.* (showing the OBD and EDR may be used to inform a driver of engine issues through a "check engine" light or to discover ways to improve gas mileage); *see also* Ralph Kisiel, *When GM designed OnStar in '95, Huber was Working Without a Map*, AUTONEWS (Sept. 14, 2018), http://www.autonews.com/article/20080914/ANA03/809150441/when-gm-designed-onstar-in-95-huber-was-working-without-a-map (highlighting that in 1996 GM added OnStar, a cellular data link which allows customers to unlock the vehicle remotely or alert first responders).

13 *See* Arun Ganesan, *Data Security and Privacy in the Connected Car Age*, ELEC. COMPONENT NEWS (Aug. 15, 2018), https://www.ecnmag.com/article/2018/08/data-security-and-privacy-connected-car-age (explaining vehicles analyze patterns, driving habits, and histories of the drivers); *see also* John R. Quain, *Cars Suck Up Data About You. Where Does It All Go?*, N.Y. TIMES (July 27, 2017), https://www.nytimes.com/2017/07/27/automobiles/wheels/car-data-tracking.html (defining recorded personal information as driver's eye movements, phone calls, texts, contact information, travel history, online search history, application usage, and violations of traffic laws).

14 *See* Jake Lingeman, *What Is Infotainment?*, AUTOWEEK (June 8, 2017), https://autoweek.com/article/technology/what-infotainment-autoweek-explains (explaining an infotainment system is the central screen in one's car associated with radio, media, and navigation functions allowing for communication, entertainment, and data collection).

15 *See* Quain, *supra* note 13 (explaining car companies want to access more data like your car's video cameras to see what you see when driving down a street).

16 Sean O'Kane, *How Tesla and Waymo are Tackling a Major Problem*

are installed with "eight cameras, 12 ultrasonic sensors, and one forward-facing radar."[17] The data collected by the cameras and sensors is used to determine what consumers want and use their vehicles for.[18] Additionally, the information collected from one's everyday use of the vehicle is freely given up to the car manufacturer or owner of the data device.[19]

B. Connected Vehicle Technology: V2V, V2I, and CVMA

Connected vehicles communicate in three different ways: vehicle-to-vehicle ("V2V"), vehicle-to-infrastructure ("V2I"), and Connected Vehicle Mobility Applications ("CVMAs").[20] V2V communication technology is primarily utilized for crash avoidance.[21] For example, one might hear a beep, see a flashing light in the dash, or feel a vibration from the seat and steering wheel if his or her vehicle is too close to another vehicle or object.[22]

Similarly, V2I communication technology "involves the exchange of safety and operational data between vehicles and elements of the transportation infrastructure."[23] This prevents accidents and creates notice of possible dangerous situations via a

---

for Self-Driving Cars: Data, VERGE (Apr. 19, 2018) https://www.theverge.com/transportation/2018/4/19/17204044/tesla-waymo-self-driving-car-data-simulation (explaining Waymo's vehicles have "three different types of LIDAR sensors, five radar sensors, 12 ultrasonic sensors, and one forward-facing radar").

17 *Id.*

18 *See id.* (stating "Tesla has access to data about the car's speed, acceleration, braking, battery use, and can save 'short video clips' during accidents [per] the company's privacy policy.").

19 *See* Tesla: Privacy & Legal, *Customer Privacy Policy* (Nov. 25, 2018), [hereinafter "Tesla Policy"] https://www.tesla.com/about/legal (stating "[b]y providing information to us or by using our products or services" the consumer agrees to Tesla's privacy policy).

20 *See* Dorothy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J. 1617, 1627-28 (2016); *see also* Brandon Amon, *Invading the Driver's Seat: Preventing Overbearing Targeted Advertising in Connected Vehicles*, 46 HOFSTRA L. REV. 329, 334-43 (2018) (providing an in-depth discussion of V2V, V2I, and CVMA technology).

21 *See* Glancy, *supra* note 20, at 1627-28; 1632 (stating the V2V receiver works through a communication spectrum between vehicles which sends and receives "360-degree" safety data).

22 *Id.* at 1632.

23 UNITED STATES DEPARTMENT OF TRANSPORTATION, VEHICLE-TO-INFRASTRUCTURE (V2I) PROGRAM 1 (2016), http://www.its.dot.gov/factsheets/pdf/JPO-17-442-V2I-Program.pdf.

vehicle's interaction with the infrastructure on the roads, such as traffic lights and safety signs.[24]

Further, CVMAs enhance convenience, information, and entertainment when a person connects or "plugs in" his or her smartphone to a vehicle's infotainment system.[25] Once connected to the infotainment system, a person may access applications for navigation, music, phone calls, and text messaging.[26] A person may also receive suggestions based on phone use and driving habits much like advertisement suggestions on Facebook and Instagram.[27] Finally, automakers developed "embedded" connections which connect a person to the internet though Wi-Fi hardware installed in the automobile.[28]

C. Data Privacy Regulations: The GDPR and CCPA

The United States does not have an automotive data privacy federal regulation.[29] Rather manufacturers must comply with the GDPR internationally and the CCPA nationally.[30]

---

24 Amon, *supra* note 20, at 339.

25 *See* Glancy, *supra* note 20, at 1636 (stating CVMA enhances vehicle experiences with navigation advice and traffic reports); *see generally* Christopher Hill, *Module 13: Connected Vehicles* (2015), http://www.pcb.its.dot.gov/eprimer/documents/module13.pdf.

26 *See* Glancy, *supra* note 20, at 1636; *see also* Amon, *supra* note 20, at 340-41 (showing CVMA enables an enhanced and efficient driving experience and keeps tabs on vehicle performance).

27 *Id.*; *see* Laura Forer, *The Complete Guide to Facebook and Instagram Advertising Targeting Options*, MKTG. PROF. (Aug. 31, 2017), https://www.marketingprofs.com/chirp/2017/32619/the-complete-guide-to-facebook-and-instagram-advertising-targeting-options-infographic ("120 million Instagrammers got in touch with a business as a result of an ad.").

28 Amon, *supra* note 20, at 340; *see also* Andrew Meola, *Automotive Industry Trends: IoT Connected Smart Cars & Vehicles*, BUS. INSIDER (Oct. 6, 2016), http://www.businessinsider .com/internet-of-things-connected-smart-cars-2016-10 (showing that embedded cars utilize an in-car antenna and chipset).

29 *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/ (explaining the need for a federal regulation); *see also* Jon Brodkin, *Sen. Marco Rubio Wants to Ban States From Protecting Consumer Privacy*, ARS TECHNICA (Jan. 18, 2019), https://arstechnica.com/tech-policy/2019/01/sen-marco-rubio-wants-to-ban-states-from-protecting-consumer-privacy/ (discussing the American Data Dissemination Act).

30 *See* 2016 O.J. (L 119) 1 (providing legislation on the protection of

The GDPR is a European Union regulation that applies to the processing of personal data that is automated or part of a filing system.[31] Consumer's rights include: (1) information notices; and (2) access right.[32] Additionally, consumers have the right to consent to data use and have a right to be forgotten.[33] Businesses must report data breaches within 72 hours of detection, utilize privacy impact assessments, and appoint a Data Protection Officer.[34] When a company fails to comply with the GDPR, noncompliance can lead to penalties as high as twenty million euros or four percent of the company's annual global turnover, whichever is higher.[35]

Domestically, manufacturers must comply with the CCPA, which took effect on January 1, 2020.[36] The CCPA applies to any organization that conducts business in California and satisfies one of three conditions: (1) annual gross revenue in excess of $25 million; (2) annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes the personal

---

personal data); *see also* Cal. Civ. Code §§ 1798.100-1798.198 (operative Jan. 1, 2020) (regarding legislation of consumer rights on collection of personal information by businesses).

31 2016 O.J. (L 119) 1 art. 2 (stating "[t]his Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.").

32 *Id.* art. 12-22; *see also General Data Protection Regulation Guide*, JONES DAY 1, 5-6, https://www.jonesday.com/files/upload/GDPR%20Pocket%20Guide%20A5%2004_17_18%20ENGLISH.pdf (showing the GDPR requires notice, access right, and the right to be forgotten).

33 2016 O.J. (L 119) 1 art. 12, 17; *see also* Yoav Levy, *What does the GDPR have to do with Car OEMs?*, UPSTREAM https://www.upstream.auto/blog/dgpr/ (last visited Aug. 25, 2019) (explaining the GDPR applies to vehicles because car companies collect personal data like diagnostics, infotainment systems, and embedded SIM cards).

34 2016 O.J. (L 119) 1 art. 33.

35 *Id.* art. 83, 84.

36 CAL. CIV. CODE §§ 1798.100-1798.198 (operative Jan. 1, 2020); *see also* Alexander H. Southwell et al., *California Consumer Privacy Act of 2018*, GIBSON DUNN (July 12, 2018) (stating the CCPA takes effect on January 1, 2020 and aims to increase transparency and control how companies utilize personal data); Sarah Meyer, *CCPA Compliance Poses Significant Challenges for U.S. Companies*, CPO MAG. (Oct. 29, 2018), https://www.cpomagazine.com/2018/10/29/ccpa-compliance-poses-significant-challenges-for-us-companies/.

information of 50,000 or more consumers, households, or devices, alone or in combination; or (3) derives 50 percent or more of its annual revenue from selling consumers' personal information.[37]

Under the CCPA, businesses must give consumers the option to opt-out of data sharing, must provide consumers with access to their information, and must delete consumer data upon request.[38] However, a business does not have to delete consumer data if it "is necessary" to: (1) complete the transaction for which the data was collected; (2) provide a consumer requested good or service; (3) perform contractual obligations; (4) detect security issues; (4) protect against "malicious, deceptive, fraudulent, or illegal" activities; (5) prosecute people for acting in a "malicious, deceptive, fraudulent, or illegal" manner; and (6) allow the business to exercise another lawfully created right.[39]

In addition, manufacturers must comply with the Federal Trade Commission's Fair Information Practice Principles ("FIPPs").[40] Under FIPPs, automakers commit to: (1) provide customers with clear, meaningful information about the information collected and how it is used; (2) provide ways for customers to manage their data; and (3) obtain affirmative consent before using geolocation, biometric, or driver behavior information for marketing and before sharing that information with third parties for personal use.[41] Even though FIPPs is used as more of a guideline, automotive companies such as Tesla[42] and GM[43] abide by the principles in

37 CAL. CIV. CODE § 1798.140(c)(1) (operative Jan. 1, 2020); *see California Consumer Privacy Act of 2018*, SULLIVAN & CROMWELL (July 2, 2018), https://www.sullcrom.com/files/upload/SC-Publication-New-Statute-Introduces-Privacy-Protections-for-California-Consumers-and-Subjects-Businesses-to-Potential-Liability.pdf (showing the CCPA establishes a new privacy framework for "Covered Businesses").

38 CAL. CIV. CODE §§ 1798.100(d), 1798.105(a), 1798.120(a) (operative Jan. 1, 2020).

39 *Id.* § 1798.105(d).

40 *See* DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, Ch. IV (1973) ("Recommended Safeguards for Administrative Personal Data Systems").

41 *Id.*

42 *See* Tesla Policy, *supra* note 19 (using Tesla's products, Tesla may collect "(1) information from or about you or your devices; (2) information from or about your Tesla vehicle; and (3) information from or about your Tesla energy products.").

43 *See General Motors: Privacy Statement*, (last visited Oct 2019), https://www.gm.com/privacy-statement.html [hereinafter "GM Policy"] (stating GM may "keep [a consumer's] information for as long as necessary" and may use information "to provide products and services,

their privacy policies because the principles may be enforceable through the Federal Trade Commission Act and other consumer protection laws.[44]

D. How are Consumers and Automobile Companies Impacted?

Consumers may be impacted when purchasing a new car, signing a contract for the car, and then later finding that the car company is syphoning the new car owner's personal data.[45] Based on the signed contract, the car company may store and use information ranging from how hard a person brakes to a person's favorite restaurant.[46]

Presently, auto manufacturers and other third-party companies may monitor a person's travel to create advertisement profiles for in-car advertising.[47] Moreover, a vehicle's route could be calculated in a way that the driver is navigated towards a specific area in hopes that the driver will stop and make a purchase along the way.[48] This unlimited access to a person's life may lead to privacy

---

to maintain customer relationships, for safety and product research purposes," for user support, and marketing).

44 *See* 15 U.S.C. §§ 41-58 (2019) (explaining businesses must adhere to practices that protect a consumer's personal information); *see also NIST Launches Privacy Framework Effort*, HUNTON ANDREWS KURTH (Sept. 11, 2018), https://www.huntonprivacyblog.com/2018/09/11/nist-launches-privacy-framework-effort/#more-16810 (showing a compliance framework).

45 Holley, *supra* note 3.

46 *Id.*

47 *See* Gabrielle Coppola & David Welch, *Pop-up ads in your car? It could be the Next Big Thing?*, CHIC. TRIB. (Mar. 6, 2018), https://www.chicagotribune.com/classified/automotive/sc-auto-cover-in-car-advertising-20180305-story.html (discussing an e-commerce system that lets drivers order coffee or make restaurant reservations while driving); *see also* Andrew J. Hawkins, *GM's Data Mining is just the Beginning of the in-car Advertising Blitz*, VERGE (Oct. 17, 2018), https://www.theverge.com/2018/10/17/17990052/gm-radio-listen-tracking-habits-advertising-future/ (showing how technological advancements allow companies to gather data. GM developed an in-car advertiser technology that lets drivers order coffee or make reservations while driving.).

48 *See* William J. Kohler & Alex Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles*, 31 SANTA CLARA COMPUT. & HIGH TECH. L.J. 99, 122-24 (2015) (showing a vehicle's route, based on past driving and

concerns related to a trip to the doctor, a religious location, a friend's home, etc.[49]

Automotive companies and third parties are positively impacted from the offset.[50] The collected data is of great monetary interest in the auto industry, and there are many reasons that automakers collect data.[51] First, data is collected for safety and maintenance purposes via EDRs and OBD-II.[52] Second, data is scraped from the infotainment system to better understand the automotive consumer's needs.[53] This is for both monetary purposes and for creating a vehicle that directly impacts a consumer's needs and wants.[54]

Finally, third parties utilize dongles that connect to a port in a car which collects information about the vehicle, driver behavior, and app-based information which includes geolocation, navigation, etc.[55] While companies benefit from data collecting, companies could face negative impacts when storing and utilizing a person's automotive data without permission or when data is illegally obtained through a hack or breach.[56]

i. Automotive Companies Must Comply with Privacy Regulations

---

purchasing habits, could be planned so that it happens to go by the business that is paying for the in-car advertisements).

49 *Id.* at 122-23 n.140 (citing People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)) (stating an automotive company's access to data and navigation may lead to discovery of more private data).

50 *See* Holley, *supra* note 3 (showing data can enhance in-car experiences with a unique driver profile and reduce accidents).

51 *See* Ganesan, *supra* note 13 (explaining connected vehicles have the power "equivalent of 20 computers" and the collected data will soon be more valuable than the car sale itself).

52 *See id.* (stating there are over a dozen sensors used to capture data from one's vehicle).

53 *See id.* (explaining data collected from one's infotainment center gives a manufacturer access to a consumer's favorite songs or favorite coffee shop).

54 *See id.* (showing the collected data may be used to pay tolls or to gain benefits from the consumer's insurance company by showing that the consumer has good driving habits).

55 *See* Edelstein, *supra* note 10 (explaining a "dongle" "[P]lugs into the OBD-II port and connects wirelessly to a network").

56 *See* 2016 O.J. (L 119) 1 art. 84 (stating a consumer could receive a remedy when a business fails to comply with the GDPR's provisions regarding privacy policies and data breaches); *see also* Cal. Civ. Code § 1798.150 (stating a consumer could bring a private right of action if actual damages are shown).

Automotive corporations, manufactures, and third-parties are impacted on a grander level when they fail to comply with privacy regulations.[57] For example, companies must receive consent before utilizing a person's "likeness" to sell products or services.[58] In *Fraley v. Facebook, Inc.,* the court held that the plaintiff showed actual injury where Facebook utilized the plaintiffs' "likeness" without full disclosure and consent when Facebook sponsored stories and misappropriated users' names and likeness for commercial endorsement.[59] Here, Facebook gained revenue by allowing advertisers to place targeted ads on a user's page.[60]

In addition, in *In re Carrier IQ, Inc., Consumer Privacy Litigation*, the Northern District of California held that providers, not carriers, may only be protected from liability when "the providers were monitoring communications for the purposes of ensuring that the providers could appropriately route, terminate, and manage messages."[61] Carrier IQ, one of the defendants, agreed to settle based on invasion of privacy allegations when it was given permission which allowed recording of everything, ranging from keystrokes to phone calls on a person's cell phone.[62] The cell phone use recording was basically undetectable and was done without the consumer's permission.[63]

Further, in *In re Google, Inc. Privacy Policy Litigation,* the Northern District of California reasoned plaintiffs must show

---

57 *See* LegalEase Solutions, *How Automotive Companies Should Respond to GDPR, CCPA, and Other International Privacy Laws*, LEGALEASE SOLUTIONS (last visited Oct. 21 2019), https://www.legaleasesolutions.com/whitepapers/how-automotive-companies-should-respond (addressing new privacy legislation that affects all industries in Europe and soon US).

58 *See* Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 806 (N.D. Cal. 2011) (reasoning plaintiffs must consent to their likeness being used by Facebook).

59 *See id.* at 804-805 (reasoning the newsworthiness exception to a commercial misappropriation claim does not apply if the publication was for commercial advertising purposes).

60 *Id.* at 790 (arguing that the sponsored ads misappropriated the users' likeness because it allowed others to assume that the plaintiff "like[d]" the advertisement because the ad appeared on the plaintiff's page).

61 *In re* Carrier IQ, Inc., Consumer Privacy Litigation, 78 F. Supp. 3d 1051, 1085 (N.D. Cal. 2015).

62 *See id.* at 1062 (showing plaintiffs allegations that defendant collected various amounts of data inputted by plaintiffs).

63 *Id.* at 1060.

actual injury when a company uses, "comingles," or gives a third-party access to a person's personal data.[64] Plaintiffs failed to show actual injury when arguing that Google violated its privacy policy which promised to use collected data only for that particular Google product.[65]

Finally, the Ninth Circuit in *Cahen v. Toyota Motor Corporation* held the car owners did not sufficiently allege an injury due to privacy invasion because the owners did not show that the data collected from their vehicles "[was] sensitive or individually identifiable. . . ."[66] In short, plaintiffs failed to show that their vehicles had actually been hacked.[67] Merely alleging vulnerability to a hack is not sufficient.[68] Thus, companies face liability when failing to be upfront about data usage.[69]

ii. What is a Data Breach?

A data breach is "a security incident in which information is accessed without authorization."[70] Recently, many car companies

64 *In re* Google Inc. Privacy Policy Litig., 58 F. Supp. 3d 968, 977-79 (N.D. Cal. 2014) (alleging Google "commingled" user data from Google platforms and disclosed the data to third parties).

65 *See id.* at 974-89 (dismissing plaintiffs' claims for failing to (1) allege that they purchased replacement phones to escape Google's new policy; (2) cite any supporting authority showing that a provider cannot violate limitations imposed by its own privacy policy; and (3) allege Google used plaintiffs' names, voices, signatures, photographs, or likeness without their consent); *see also* Bloomberg Law: Privacy & Data Security, *Court Dismisses Google Privacy Policy Case; Data Disclosure Note Enough for Standing* (Jan. 7, 2013), https://www.bna.com /court-dismisses-google-n17179871721/ (explaining plaintiffs failed to allege concrete harm).

66 Cahen v. Toyota, 717 Fed. App'x. 720, 723-24 (9th Cir. 2017).

67 *See id.* (indicating plaintiffs filed a class action against Ford, GM, and Toyota alleging the defendants left plaintiffs susceptible to hack due to the automotive technology and defendants improperly collected and transmitted their personal information).

68 *See Cahen*, 717 Fed. App'x. 720 at 724 (discussing merely alleging hack vulnerability is insufficient).

69 *See* Orson Lucas, *Driving Change*, KPMG LLP (2018), https://advisory.kpmg.us/content/ dam/advisory/en/pdfs/driving-change.pdf (stating businesses must ensure consumers are informed).

70 Norton, *What is a data breach?* (2018), https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html.

such as Tesla and Toyota suffered major data breaches due to a third-party manufacturer's lack of security which exposed 47,000 documents including corporate documents such as blueprints, client invoices, and nondisclosure agreements.[71]

Similarly, in 2018, Facebook discovered a security breach which impacted 50 million users.[72] Following Facebook's breach announcement, individuals filed a class action alleging Facebook was responsible for this "massive breach" after failing to adequately secure users' personal information.[73] This breach occurred not long after the Cambridge Analytica controversy, which led to the unauthorized data mining of millions of Facebook users information.[74]

In the same way, Uber was hacked twice within a two-year period and failed to immediately disclose the data breach.[75] In

71 Stacy Cowley, *'Big Red Flag': Automakers' Trade Secrets Exposed in Data Leak*, N.Y. TIMES (July 20, 2018), https://www.nytimes.com/2018/07/20/business/suppliers-data-leak-automakers.html; *see* Kirsten Korosec, *Data Breach Exposes Trade Secrets of Carmakers GM, Ford, Tesla, Toyota*, TECHCRUNCH (July, 21, 2018), https://techcrunch.com/2018/07/20/data-breach-level-one-automakers/ (last visited Feb. 17, 2019) (Tesla and Toyota were exposed on a publicly accessible server belonging to Level One Robotics); *see also* Mike Murphy, *A New Data Breach May Have Exposed Personal Information of Almost Every American Adult*, MARKETWATCH (June 28, 2018, 8:19 AM), https://www.marketwatch.com/story/a-new-data-breach-may-have-exposed-personal-information-of-almost-every-american-adult-2018-06-27 (showing a third-party data company was hacked exposing 3.5 billion consumer information ranging from automotive to behavioral data).

72 *See* Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018) https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (showing law enforcement were informed three days after the breach was noticed); *see also* Guy Rosen, *Security Update*, FACEBOOK NEWSROOM (Sept. 28, 2018), https://newsroom.fb.com/news/2018/09/security-update/ (notifying Facebook users of the security breach).

73 Class Action Complaint at 6, 9-10, Echavarria v. Facebook, Inc., No. 5-18-cv-05982 (N.D. Cal. filed Sept. 28, 2018) (including "names, email address, recovery email accounts, telephone numbers, birthdates, passwords, and security question answers").

74 *See* Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (showing more than fifty million Facebook user's information was harvested allowing the exploitation of each user's private social media activity).

75 Complaint at 1, 5-7, *In re* Uber Techs., Docket No. C-4662 at 1, 5-7

2014, Uber was hacked exposing over 100,000 drivers' personal data.[76] In 2016, Uber paid the hackers $100,000 to delete the data and "keep quiet" when the hackers stole 57 million Uber users' and drivers' personal data.[77] The FTC argued that Uber failed to protect Uber riders' and drivers' personal information and to inform riders and drivers of the breach.[78] Uber agreed to implement a comprehensive privacy program, conduct and provide the FTC with third-party privacy audits for twenty years, retain records of bug bounty reports, and be honest about its privacy measures.[79]

Further in 2015, Anthem incurred a data breach of 78.8 million insured's Personally Identifiable Information ("PII") and Personal Health Information ("PHI"), which included social security numbers and health data.[80] The complaint alleged that Anthem failed to take adequate and reasonable measures to ensure data systems protection, failed to take steps to prevent and stop the breach from happening, and failed to disclose to its customers that its system and security practices were inadequate to safeguard personal data.[81]

Finally, Marriott is currently under investigation for a hack that involved 383 million guest records exposing 5.25 million unencrypted passport numbers, and 20.3 million encrypted passport numbers.[82] While the case has not been decided, multiple

---

(F.T.C. Oct. 25, 2018); *see also* Liam Tung, *FTC: Uber Failures Led to 2014 Hack Exposing 100k Drivers' Details*, CSO (Aug. 16, 2017) https://www.cso.com.au/article/626053/ftc-uber-failures-led-2014-hack-exposing-100k-drivers-details/ (explaining Uber noticed the hack in May 2014 and later, in May 2016, discovered more Uber users were impacted).

76 *See* Tung, *supra* note 75 (showing the hack exposed names, email address, phone numbers, trip records, driver's licenses, etc.).

77 Anita Balakrishnan & Deirdre Bosa, *Uber Hid A Hack that Exposed Data of 57 Million Users and Drivers for more Than A Year,* CNBC (Nov. 21, 2017), https://www.cnbc.com/2017/11/21/uber-hack-exposes-data-of-57-million-users-and-drivers-report-says.html.

78 *In re* Uber Techs., Inc. at 4-5, Docket No. C-4662.

79 *Id.* at 2-7 (showing Uber may not misrepresent its privacy measures).

80 *Anthem Data Breach Litigation*, COHEN MILSTEIN, https://www.cohenmilstein.com/case-study/anthem-data-breach-litigation (last visited Jan. 6, 2019).

81 *See In re Anthem Data Breach Litig.*, 162 F. Supp. 3d 953, 984-87 (N.D. Cal. 2016) (dismissing plaintiffs' claims in part to further analyze whether the defendants' actions violated public policy).

82 Yiannis Mouratidis, *GDPR May Add Up To $915 Million Marriott's*

class action suits allege that Marriott failed to protect consumer data and failed to notify consumers of the breach within a reasonable timeframe.[83] The class actions could lead to sanctions and fines amounting to $915 million for failing to enact security protocols.[84]

II. Attaining Compliance and Avoiding Liability

By 2020, less than fifteen percent of all vehicles will lack the ability to connect to the internet.[85] The potential legal implications are whether automobile companies: (1) will be able to comply with the GDPR; (2) will be able to comply with the CCPA; (3) are liable for a potential data breach; and (4) are liable for a potential privacy breach.[86]

A. GDPR Compliance – Complying with International Regulations

The GDPR applies to automotive businesses because connected vehicles process "personal data" such as diagnostics, event data recorders, and location.[87] GDPR compliance is attained by

---

Data Breach Expenses, at 1-2, FORBES (Jan. 9, 2019) https://www.forbes.com/sites/yiannismouratidis/2019/01/09/gdpr-may-add-up-to-8-8b-marriotts-data-breach-expenses/#57541b1562e1.

83 *See id.* (explaining the Marriott case status); *see also* Bell v. Marriott International, Inc., 8:18-cv-03684-PX 1 (D.C. MD Nov. 30, 2018).

84 *See* Mouratidis, *supra* note 82 (showing the GDPR may increase the fines imposed on Marriott by four percent of its annual revenue for failing to enact sufficient security protocols).

85 *See* Stephen Lawson, *5G Cars Coming in 2020, Joining Wave of Connected Vehicles*, AUTO.: CONNECTED VEHICLES (July 19, 2018), https://www.tu-auto.com/5g-cars-coming-in-2020-joining-wave-of-connected-vehicles/ (showing between 2018 and 2022 there will be more than 125 million connected vehicles).

86 *See* Jeewon Serrato, *Connected Cars and Data Privacy: Global Regulatory Challenges*, SHEARMAN & STERLING LLP (2017) (explaining the automotive industry needs to conduct privacy assessments and maintain compliance with privacy regulations).

87 Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(1), 2016 O.J. (L 119) 1 (defining personal data as information related to an identified or identifiable person); *see also General Data Protection Regulation Guide*, *supra* note 32, at 2 (stating GDPR applies when

developing and breaking down data privacy strategies into three prongs: (1) consumers; (2) security protocols; and (3) third-parties.

i. Consumer Protection

Under the GDPR, businesses must give consumers the right to opt-in, to access the collected data, and to be forgotten.[88] Moreover, businesses must notify consumers when there is a data breach.[89]

First, a business must give consumers the chance to opt-in to data collection.[90] It is likely enough for the consumer to opt-in by using the vehicle.[91] The court in *Fraley* reasoned that even if a user does not read Facebook's policy, Facebook may place the user's "likes" on a Sponsored Story because the user consents or opts-in to the use of their "likeness" by using Facebook and by knowingly choosing to "like" posts on the website.[92] In the same way, a court will likely reason that if a user fails to read an automaker's policy, the automaker may utilize the user's collected data because the user has opted-in by using the vehicle.[93]

Nevertheless, to comply with the GDPR, a business would benefit from giving consumers the chance to knowledgably opt-in

---

processing personal data).

88 *See* Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 15, 17-18, 2016 O.J. (L 119) 1; *see also* Kris Lahiri, *What is General Data Protection Regulation?*, FORBES (Feb. 14, 2018), https://www.forbes.com/sites/quora/2018/02/14/what-is-general-data-protection-regulation/#d2b2a3262dd8 (showing a company offering goods or services and monitoring consumer's data must be GDPR compliant).

89 *See* Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 33, 2016 O.J. (L 119) 1.

90 *See id.* art. 12.

91 *See* Fraley v. Facebook, Inc., 966 F. Supp. 2d 939, 942 (N.D. Cal. 2013) (reasoning Facebook users understand using Facebook and "liking" posts lead to the "liked" posts showing up on other users' feeds).

92 *See id.* (explaining plaintiffs failed to show harm when Facebook used plaintiffs' "likeness" in the Sponsored Stories).

93 *See id.* (discussing Facebook "does nothing more than take information users have already *voluntarily* disclosed to their 'friends,' and sometimes redisplays" that information).

to this collection.[94] For example, when a business utilizes consumers' vehicle GPS data, consumers must understand what the data is ultimately being used for prior to opting-in to the collection.[95] Thus, to avoid investigations and looming GDPR fines, businesses must ensure that consumers understand what data is collected, why the data is collected, and how the data is collected.[96]

An automobile manufacturer can avoid a Facebook Cambridge Analytica scandal by laying out all aspects of the data collection process in the consumer's contract.[97] In the Cambridge Analytica scandal, Facebook failed to inform users that it was mapping users' personality traits to generate targeted ads by collecting details of their identities, friend networks, and "likes."[98] Similarly, an automaker will likely face consequences if it fails to keep consumer's informed when it utilizes consumer's GPS and infotainment data to create targeted ads for companies like Starbucks or Dominos.[99]

In contrast to the consent needed in *Fraley* where a user merely needed to use the service and have a general understanding of how Facebook "likes" work, in the auto industry, a user likely needs to use the service and have a general understanding of what data is being collected.[100] The user understands that by liking a page, the

94 *See* 2016 O.J. (L 119) 1 art. 12 (explaining what information users must be given upon request under the GDPR); *see also General Data Protection Regulation Guide*, *supra* note 32, at 3, 9 (explaining the company and consumer agreement must be freely agreed to, have "clearly discernible" consent, and the consumer must be knowledgeable regarding why the data is used).

95 *See General Data Protection Regulation Guide*, *supra* note 32, at 5 (showing a consumer must have access to concise and transparent information related to the data collection process).

96 *See* 2016 O.J. (L 119) 1 art. 77 (stating that people whose data has been collected have administrative remedies available); *see also Uber Techs.*, *supra* note 75, at 4-7 (showing that companies should have transparent and accurate privacy policies).

97 *See* 2016 O.J. (L 119) 1 art. 13-14 (providing a list of information that data subjects must be given, subject to some exceptions); *see also* Rosenberg, *supra* note 74 (showing that out of 50 million Facebook profiles, roughly 270,000 users consented to having their data harvested).

98 Rosenberg, *supra* note 74 (explaining the methods used by Cambridge University researchers to collect users' data).

99 *See* 2016 O.J. (L 119) 1 art. 13 (explaining when consumers must be notified regarding the collection and use of the consumer's data); *see also* Rosenberg, *supra* note 74 (showing users must be informed of how Facebook uses consumer data).

100 *See* Fraley v. Facebook, Inc., 966 F. Supp. 2d 939, 942-43 (N.D. Cal.

like will show up as a Facebook notification somewhere else, whether it be on the user's page, the user's feed, or a friend's page.[101] However, the data collection process is still new and a consumer is not as aware of what his or her personal data is being collected and used for.[102] Thus, a business must go a step forward from the *Fraley* analysis and inform consumers of the data collection process before the consumer consents.[103]

Second, businesses must give consumers the right to access the personal data that is collected.[104] This means that the consumer may ask for copies of the collected data and receive information about how the data is collected and used.[105] In contrast to Tesla's policy on a consumers right to access,[106] to comply with the GDPR, the business must ensure that a consumer understands he or she has the right to access their personal information.[107]

Just as consumers have the right to access, consumers have the right to be forgotten.[108] This is a bit of a misnomer as data may be

---

2013) (reasoning plaintiffs had a hard time proving no express or implied consent).

101 *See Fraley*, 966 F. Supp. 2d at 942 (stating Facebook users, even without reading the policy statements, typically understand that their "likes" will appear on other's newsfeeds).

102 *See* Quain, *supra* note 13 (explaining the driver, when using an application, generally agrees to agreement terms by checking a box within the vehicle's infotainment or navigation system).

103 *See Fraley*, 966 F. Supp. 2d at 942 (showing users merely need to use Facebook and generally understand how Facebook works); *see also* Rosenberg, *supra* note 74 (explaining Facebook users must be informed of how Facebook uses consumer data).

104 *See* Commission Regulation 2016/679, art. 15, 2016 O.J. (L 119) 1, 43 (EU) (stating the consumer has the right to access information such as "the purposes of the processing; the categories of personal data concerned;" the recipients of who might receive the consumer's data).

105 *See id.*(explaining data subjects have the right to access their data); *see also* JONES DAY, *supra* note 32, at 5 (stating "[d]ata subjects have the right to obtain copies of their personal data, along with key details about how the data is processed.").

106 *See* Tesla Policy, *supra* note 19 (stating "you may have the rights to request access to and receive information about certain information . . . ; update and correct inaccuracies in that information; have the information restricted or deleted; object or withdraw your consent to certain uses of information; and lodge a complaint with your local supervisory authority").

107 *See* Commission Regulation 2016/679, art. 15, 2016 O.J. (L 119) 1, 43 (stating consumers have the right to access their information).

108 *See* Commission Regulation 2016/679, art. 17 2016 O.J. (L 119) 1, 43-44 (explaining consumers have the right to have their personal information erased); *see generally* Daphne Keller, *The Right Tools:*

accessed again even if it is completely deleted or "forgotten."[109] Businesses would benefit from ensuring a timely protocol that allows consumers to understand: (1) the data deletion process; (2) what data still remains after deletion; (3) why data is not deleted; and (4) the appeals process.[110]

Finally, businesses must notify consumers within seventy-two hours of detecting a data breach.[111] This can be a difficult process because businesses are stuck between covering their bases and protecting the consumer.[112] Here, transparency is key; businesses should educate the consumers of all of the details reasonably necessary to inform each consumer of what data was breached and how it impacts the consumer.[113]

Even though a business must only inform a consumer of a personal data breach if it is likely to result in a "high risk" to the person's rights, a business could avoid investigations and fines if it puts the consumer's needs above business needs.[114] For example,

---

Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, 33 BERKELEY TECH. L.J. 289, 326 (2018), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwjE3pzXpr3lAhUnx1kKHcwMAnwQFjABegQIAhAC&url=http%3A%2F%2Fbtlj.org%2Fdata%2Farticles2018%2Fvol33%2F33_1%2FKeller_Web.pdf&usg=AOvVaw2xmH2KM_7qo4fNSV3ql3wn (explaining the GDPR is unclear on whether a host site such as Facebook is required to take down a user's information when a user tries to enforce his or her right to be forgotten).

109 *See* Rosenberg, *supra* note 74 (showing Facebook explained that post-hack not all data was deleted even though there were certifications that stated otherwise); *see also* Tribune Wire Reports, *Experts: Deleted Online Information Never Actually Goes Away*, CHIC. TRIB. (Aug. 21, 2015, https://www.chicagotribune.com/bluesky/technology/chi-deleted-online-information-never-goes-away-20150821-story.html (stating it is unlikely that any information is permanently deleted).

110 2016 O.J. (L 119) 1 art. 17(1)-(3).

111 *Id.* art. 34; *see also* Shawn Ryan, *72 Hours: Understanding the GDPR Data Breach Reporting Timeline*, IMPERVA (May 16, 2018), https://www.imperva.com/blog/72-hours-understanding-the-gdpr-data-breach-reporting-timeline/ (showing once notified, the business must conduct an investigation, inform impacted parties, and explain what data was breached).

112 *See In re* Uber Techs. Inc., No. C-4662, 2018 FTC LEXIS 166, at 1 (Oct. 25, 2018) (showing Uber chose to pay off hackers rather than inform consumers).

113 2016 O.J. (L 119) 1 art. 17(1)-(3); *see also* Ryan, *supra* note 111 (showing the business must inform consumers of the nature of the breach, the impact and consequences of the breach, and the measures taken to mitigate the breach).

114 2016 O.J. (L 119) 1 art. 34(1); *see In re* Matter of Uber Techs., Inc.,

assume that a hacker infiltrates one consumer's vehicle via its V2I technology, and is able to access all surrounding vehicles through a hole in the V2V and V2I technology.[115] A business must inform consumers of the hack and must not hide the hack in hopes of fixing the problem before the public finds out.[116]

ii. Security Protocols

Marriott is facing the possibility of sanctions and fines that could amount to $915 million for failing to enact security protocols, failing to disclose within a reasonable time period, and causing serious losses for its investors.[117] Likewise, the auto business could face similar sanctions and fines.[118] In 2015, hackers gained control of a car's brakes and turned off the engine via a Jeep's V2V system.[119]

Based on this incident, and with the Marriott breach in mind, Jeep could be the subject of multiple lawsuits for failing to adequately protect consumer information and for failing to notify consumers within a reasonable time period not to exceed 72 hours from the breach.[120] Specifically, under the GDPR a consumer may

---

No. C-4662, 2018 FTC LEXIS 166, at 1 (Oct. 25, 2018) (explaining Uber hid the hack by paying off the hackers rather than informing consumers).

115 *See* Liam Tung, *VW-Audi security: Multiple Infotainment Flaw Could Give Attackers Remote Access*, ZDNet (May 1, 2018), https://www.zdnet.com/article/vw-audi-security-multiple-infotainment-flaws-could-give-attackers-remote-access/ (showing hackers may access information through a network flaw).

116 2016 O.J. (L 119) 1 art. 17(1)-(3); *see also* Todd M. Hinnen et al., *GDPR Data Breach Notification Requirements*, PERKINS COIE LLP (May 25, 2018), https://www.perkinscoie.com /print/content/25194/gdpr.pdf (reasoning once a breach is found, a company must notify the supervising authority, any third-party "without undue delay," and the impacted consumers).

117 Mouratidis, *supra* note 82.

118 *Id.*; *see also* Zack Whittacker, *Hackers Can Take Over Your Jeep, Literally Driving You Off the Road*, ZDNET (July 21, 2015), https://www.zdnet.com/article/fiat-chrysler-bug-hackers-can-literally-drive-you-off-the-road/.

119 Whittaker, *supra* note 118; *see also* Tung, *supra* note 115 (explaining hackers found security flaws in VW and Audi vehicles' infotainment systems that could lead to the collection of a consumer's data).

120 *See* 2016 O.J. (L 119) 1 art. 34, 8 art. 79(1); *see also* Seena Gressin, *The Marriott Data Breach*, FTC: CONSUMER INFO. (Dec. 4, 2018) https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach

seek a judicial remedy at any time when the consumer feels that his or her rights have been infringed.[121] This means that a business may be the subject of a lawsuit anytime a consumer notices that a business fails to grant access to the user's personal data, to remove information requested by the user, or to adequately state within the privacy policy how the user's information is protected.[122]

To avoid a Marriott-like situation and to maintain GDPR privacy compliance, businesses must conduct mandatory privacy impact assessments and appoint a Data Protection Officer.[123] Further, businesses will need to ensure that there are effective security measures in place to protect consumers.[124] For example, Uber was subject to extensive audits when Uber failed to conduct privacy impact assessments and failed to enact security protocols to protect consumers.[125] Similarly, an automaker could be subject to fines and audits if the automaker fails to conduct privacy impact assessments ensuring consumer data security and fails to create a security protocol that adequately explains how the consumer's data is protected.[126]

In addition, a businesses' privacy policy must fully reflect regulations and incorporate the what, why, and how of consumer

---

(explaining hackers accessed consumer's names, addresses, phone numbers, passport numbers, etc. through the Starwood loyalty program); *and see* Tung, *supra* note 115, (showing VW and Audi infotainment systems had vulnerabilities that allowed hackers to gain access to the vehicles).

121 2016 O.J. (L 119) 8 art. 79(1); *see also* Detlev Gabel, *Chapter 16: Remedies and Sanctions – Unlocking the EU General Data Protection Regulation*, WHITE & CASE (Apr. 5, 2016), https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection (providing a detailed analysis of the ways that a company may be sued).

122 2016 O.J. (L 119) 3 arts. 15, 17, 4 art. 25, 8 art. 79(1).

123 *Id.* at arts. 35, 37; *see also* Hinnen, *supra* note 116 (explaining there must be clear notification of a breach and the controller must keep detailed documentation).

124 2016 O.J. (L 119) 1 arts. 25, 32-35; *see also* Caitlin Gruenberg, *6 Security Controls You Need For General Data Protection Regulation*, CYBERGRX (May 17, 2018), https://www.cybergrx.com/resources/blog/6-security-controls-need-general-data-protection-regulation-gdpr/ (showing businesses must ensure security through identity and access management, data loss prevention, encryption and pseudonymization, incident response plan, third party risk management, and policy management).

125 *See In re* Uber Techs., Inc., No. C-4662, 2018 FTC LEXIS 166, at *4-7 (Oct. 25, 2018)

126 *See* 2016 O.J. (L 119) 1 art. 25, 32-35.

data collection.[127] Every consumer at the start of contractual agreements must sign the privacy policy to use the vehicle.[128] Moreover, consumers should be required to sign a new privacy policy if there are material alterations to the privacy policy.[129]

The court in *Anthem* reasoned that consumers were not adequately protected when Anthem failed to prevent and stop the breach and failed to inform its customers that Anthem's privacy and security protocols were inadequate.[130] By creating a transparent privacy policy that consumers must sign the automaker will likely avoid lawsuits for failing to adequately inform, protect, and notify consumers.[131]

iii. Third-Parties

Under the GDPR, businesses must ensure third-parties fully understand data privacy and consumer protection.[132] Meaning all

---

127 *Id.* at art. 13; *see also In re* Uber Techs., Inc., No. C-4662, 2018 FTC LEXIS 166, at *1-2 (Oct. 25, 2018) (showing Uber's privacy and security policy did not comply with its actual security protocol capabilities).
128 Chejn, *supra* note 2; *see also Example Data Protection Addendum Addressing Article 28 GDPR (Processor Terms) and Incorporating Standard Contractual Clauses for Controller to Processor Transfers of Personal Data from the EEA to a Third Country*, DLA PIPER (July 14, 2017), https://iapp.org/resources/article/sample-addendum-addressing-article-28-gdpr-and-incorporating-standard-contractual-clauses-for-controller-to-processor-transfers-of-personal-data/ (showing a GDPR compliant contract).
129 *See* Marcus Evans et al., *GDPR Checklist*, NORTON ROSE FULBRIGHT (November 2018) https://www.nortonrosefulbright.com/en/knowledge/publications/3b14a527/gdpr-checklist (showing how a business will maintain GDPR compliance by updating the privacy policy).
130 *See In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d at 987 (leaking users' information, a case that was later settled), *aff'd*, 327 F.R.D. 299, 306 (N.D.C. Cal. 2018) (affirming the fairness of the settlement).
131 *See* Evans, *supra* note 129, at 8 (explaining notice on how to handle collected data should be given to all employees and third parties).
132 *See* 2016 O.J. (L 119) 1 art. 6(1)(f) ("processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data . . . "); *see* 2016 O.J. (L 119) 1 art. 44 (stating any transfer to a "third country" or an "international organization" must comply with other GDPR provisions as well as the provisions on transfers.); *see* 2016 O.J. (L 119) 1 art. 4(26) (defining "international organization" as "an organization and its subordinate bodies governed

third-party providers must understand what data needs to be protected and how to protect it.[133] Further, to ensure third-party notice and compliance, businesses must make it clear at the beginning of contractual negotiations what data needs to be protected, what data may be shared, what data requires consumer consent, and when consumers must be notified of a data breach.[134]

B. CCPA Compliance: Complying with National Data Regulations

The CCPA will apply to automotive businesses because most auto manufacturers exceed $25 million or more annual revenue and handle more than 50,000 individual's information.[135] The CCPA and the GDPR are very similar in that consumers must have access to their information, must understand what their information is used for, and must know who may use their information.[136] Businesses can likely attain some CCPA

---

by public international law . . . ").

133 2016 O.J. (L 119) 1 art. 44; *see* Korosec, *supra* note 71 at 9 (explaining businesses are facing liability because a third-party vendor did not have adequate security measures); *see also* Murphy, *supra* note 71 (showing failure to gain third-party compliance leads to massive breaches).

134 2016 O.J. (L 119) 60 art. 44; *see also* Michael Nadeau, *General Data Protection Regulation [GDPR]: What You Need to Know to Stay Compliant*, CSO (May 29, 2019), https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html (explaining that a car company fails GDPR compliance if the third-party fails GDPR compliance).

135 CAL. CIV. CODE § 1798.140 (operative Jan. 1, 2020); *see* Sarah L. Bruno et al., *New Privacy Law Speeds Down the Highway: Implications of the California Consumer Privacy Act for Automotive Dealers*, ARENT FOX: MANAGING AUTO. BLOG (Nov. 13, 2018) https://www.arentfox.com/perspectives/managing-automotive-blog/new-privacy-law-speeds-down-highway-implications-california (explaining the four operational impacts automakers will face); *see also* I. Wagner, *Revenue of the Leading Automotive Manufacturers Worldwide in 2018 (in billion U.S. dollars)*, STATISTA, (July 23, 2019), https://www.statista.com/statistics/232958/revenue-of-the-leading-car-manufacturers-worldwide/ (showing automakers from Volkswagen to Toyota exceed $100 billion in annual revenue).

136 *Compare* CAL. CIV. CODE §§ 1798.100 to 1798.198 (operative Jan. 1, 2020) (regarding legislation of consumer rights on collection of personal information by businesses), *with* 2016 O.J. (L 119) 1 (providing legislation on the protection of personal data); *see also* Steven R. Chabinsky et al., *CCPA and GDPR: Comparison of Certain Provisions*,

compliance by following the compliance techniques outlined for the GDPR.[137] Where the CCPA and GDPR do not intersect, CCPA compliance is obtained with strict adherence to the regulation.[138]

Unlike the GDPR, which provides that consumers must opt-in, the CCPA provides that businesses must give consumers the ability to "opt-out" of sharing personal data.[139] While an opt-out process creates issues for businesses in maintaining compliance with both the GDPR and the CCPA, this creates less liability for the company.[140] For example, Tesla appears to be GDPR and CCPA compliant because its privacy policy lets a consumer opt-in to data collection merely by purchasing the vehicle and a consumer opts-out by purchasing a different car.[141]

Second, like the GDPR, consumers have a right to be forgotten and businesses must delete data upon request.[142] However, under the CCPA, the business is not required to delete consumer's information if it falls within one of the CCPA's exemptions.[143] GM

WHITE & CASE (Sep. 7, 2018), https://www.whitecase.com/publications/article/ccpa-and-gdpr-comparison-certain-provisions (comparing CCPA and GDPR scope).

137 *See* 2016 O.J. (L 119) 43 art. 15-17 (providing regulations that businesses must comply with as it relates to consumer protection); *see* 2016 O.J. (L 119) 48 art. 25 (explaining data protection protocols); *and see* 2016 O.J. (L 119) 60 art. 44 (describing the general procedure for transfers of consumer data to outside parties).

138 *See* CAL. CIV. CODE §§ 1798.100 to 1798.198 (operative Jan. 1, 2020); *see also* Bruno et al., *supra* note 135 at 16 (explaining under the CCPA, businesses must give consumers the right to opt-out to the obtained information, to be forgotten, and privacy notices must be updated).

139 *See* CAL. CIV. § 1798.185(a) (operative Jan. 1, 2020); *see also* 2016 O.J. (L 119) 1; *see also* Chabinsky, *supra* note 136 (comparing the CCPA opt-out and GDPR opt-in policy).

140 *Compare* CAL. CIV. CODE §§ 1798.100 to 1798.198 (operative Jan. 1, 2020), *with* 2016 O.J. (L 119) 1 (showing under the CCPA, consumers must opt-out while under the GDPR, consumers must opt-in); *see also* Chabinsky, *supra* note 136 (explaining the GDPR opt-in process grants consumers more rights).

141 By purchasing a Tesla, a consumer is automatically consenting to Tesla's collection and use of all information. *See* Tesla Policy, *supra* note 19 (explaining "using [Tesla's] products or services, you agree to the terms and conditions of this Privacy Policy").

142 *Id.*; *see* Robert Madge, *Five Loopholes in the GDPR*, MY DATA J. (Aug. 27, 2017) https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b (explaining the organization will process any data that it wants with the only limitation being user objections and opt-outs).

143 *See* CAL. CIV. CODE § 1798.105(d) (operative Jan. 1 2020) (stating information may be retained if "it is necessary" for business purposes).

maintains compliance with the CCPA by providing within its privacy policy the what, why, and how of its data collection process.[144] Additionally, GM meets the business related use exemption and does not have to delete any consumer data by explaining that all consumer data is used for business related purposes.[145]

In contrast, a business could face a CCPA violation for failure to delete consumer information upon request if that business does not use the information for business related reasons.[146] The plaintiffs in *In re Google* argued that Google violated its privacy policy when Google used the consumer's information in a manner inconsistent with Google's privacy policy.[147] Similarly, a consumer could argue that an auto manufacturer violated the CCPA when the business failed to delete the consumer's information as the business did not use the collected data in a business related manner.[148]

A business will likely prevail in this instance because it is unlikely that a consumer could show an actual injury related to

---

144 *See* GM Policy, *supra* note 43 ("We may collect information about you and your vehicle, such as name, address, email address, phone number, vehicle identification number (VIN) and vehicle performance data through your use of our products or services, and through GM affiliates, dealers, GM licensees for consumer merchandise, GM partners and others. . . .").

145 *See* CAL. CIV. CODE § 1798.105(d)(1) (operative Jan. 1, 2020) (explaining that the automaker meets the business purpose loophole by showing the information is necessary to "complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer"); *see also* GM Policy, *supra* note 43 (stating consumer information is used "to provide products and services, to maintain customer relationships, for safety and product research purposes," for customer support, and for marketing).

146 *See* CAL. CIV. CODE § 1798.105(a)-(d) (operative Jan. 1, 2020) ("A business that receives a verifiable request from a consumer to delete the consumer's personal information . . . shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.").

147 *See In re* Google, Inc. Privacy Policy Litig., 58 F. Supp. 3d 968, 977-79 (N.D. Cal. 2014) (arguing Google was not authorized to give third-parties access to user's data).

148 CAL. CIV. CODE §§ 1798.105(d), 1798.185(a) (operative Jan. 1, 2020); *see also* Southwell, *supra* note 36 (explaining a business may utilize a consumer's data for business related purposes).

the business' failure to delete the consumer data.[149] Moreover, a business could protect itself by stating within its privacy policy that all consumer data is collected and used for business related practices and requests for information deletion does not always erase the information.[150]

Third, businesses must update their privacy notices and policies.[151] Rather than receiving a consumer's consent through signature, Tesla's privacy policy states that it may update its policy at any time and that a consumer consents to the policy by using Tesla products or services.[152] In contrast, GM's privacy policy states that it may update its policy but does not mention consumer consent to the updates.[153]

Automotive companies must maintain transparency when informing consumers of how the company uses consumer data.[154] In the automotive industry, a consumer could argue that the automotive company violated the privacy policy the consumer previously consented to when the automotive company updates its terms of service and begins to use consumer data in a way that was not previously stated.[155] However, a company could avoid conflicts regarding its privacy policy if the consumer consents to the privacy policy every time there is an update.[156]

---

149 *See In re Google*, 58 F. Supp. 3d at 977-79 (holding the plaintiffs could not show an actual injury).
150 CAL. CIV. CODE § 1798.185(a) (operative Jan. 1, 2020); *see* GM Policy, *supra* note 43 (stating that upon request GM will grant information on how to delete obtained information; however, GM "may need to retain certain information for recordkeeping purposes, to complete any transactions that you began prior to your request, or for other purposes as required or permitted by applicable law.").
151 CAL. CIV. CODE §§ 1798.115(c), 1798.135 (operative Jan. 1, 2020); *see also* Southwell, *supra* note 36 (stating the business must update its privacy policy when disclosing consumer personal information and when giving consumers the right to opt-out).
152 *See* Tesla Policy, *supra* note 19 ("By using our products or services, or otherwise providing information to us following these changes, you accept the revised Privacy Policy.").
153 *See* GM Policy, *supra* note 43 (stating GM may update the policy from "time to time").
154 *See* Plungis, *supra* note 1 (explaining automakers "promised" to provide notice about data collection); *see also* Southwell, *supra* note 36 (stating compliance with the CCPA will require increased transparency with consumers).
155 *See In re Google*, 58 F. Supp. 3d at 978-79 (arguing that plaintiffs did not consent to Google's updated privacy policy).
156 *See* Plungis, *supra* note 1 (arguing automakers should provide consumers with complete access to the collected data and give outside

Fourth, businesses must ensure agreements with service providers and third parties are CCPA compliant.[157] Recently, companies like GM, Ford, Tesla, and VW were subject to a data breach due to a third party's lack of security.[158] It is established that companies may share consumer data with third parties.[159] However, when granting third parties access to consumer data, businesses must remain transparent.[160] Further, companies must develop security and policy regulations that the third party must conform to before the company shares the consumer collected data with the third party.[161]

Finally, businesses must train personnel to protect consumer privacy.[162] Like third party use of data, an employee has full access to a consumer's vehicle data.[163] Specifically, the employee could create a map of what the consumer does on a daily basis merely by accessing the consumer's GPS history.[164] Thus, to maintain CCPA

---

researchers access to test that consumer's data is properly used and aggregated).

157 *See* CAL. CIV. CODE § 1798.115(a) (establishing consumers may inquire into third party rights to the consumer information and how the information is used).

158 Korosec, *supra* note 71; *see also* Murphy, *supra* note 71 (highlighting a third party data company, Exactis, was hacked, which led to the exposure of over 3.5 billion consumer's information, from automotive data to behavioral data).

159 *See* In re Google, 58 F. Supp. 3d at 974 (expressing a company may share consumer information with third-parties even if the company does not state this in its privacy policy).

160 *See* Cal. Civ. Code § 1798.115 (indicating consumers must know what data is collected, how the data is used by third parties, and what data may be deleted).

161 *Id.*; *see also id.* § 1798.155 (explaining third parties may attain compliance guidance from the Attorney General on issues like curing alleged violations).

162 *Id.* § 1798.130; *see also Summary of California Consumer Privacy Act of 2018*, VENABLE LLC, http://www.aaf.org/_PDF/AAF%20Website%20Content/909_SelfRegulation/Regulatory /2018-07-31-CA_ConsumerPrivacyAct_Summary.pdf (showing businesses are required to ensure employees are trained to handle consumer information).

163 *See* Bruno et al, *supra* note 135; s*ee also* Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (describing employee access allows the employee to see a consumer's location even though data is allegedly anonymous).

164 *See id.* (stating in detail the information that is accessible based on

compliance, a company must state within its contract with the employee that all consumer data must remain a secret and may not be used for personal gain by the employee.[165] Moreover, the company must ensure the employee receives adequate training, based on the employees rank and access to consumer data.[166]

C. Data and Privacy Breach: Is the Automobile Company Liable?

Automakers must comply with privacy regulations and ensure consumer protection pre and post-data breach.[167] First, for businesses to be liable for a data breach, consumers must show an actual harm.[168] In 2017, hackers accessed consumer information by hacking into the infotainment systems of VW and Audi vehicles.[169] In this case, a consumer could establish that a hack occurred, but would likely have trouble proving harm.[170] There was no harm because the hackers did not access any consumer information, but only moved through the vehicle system to expose security vulnerabilities.[171]

Second, a business is likely liable if it does not have adequate privacy protocols and safeguards in place to protect the consumer's

---

the data that companies use and analyze).

165 *See CCPA Organizational Readiness Checklist*, CENTRL, https://www.oncentrl.com/CCPA-organizational-readiness-checklist (last visited Apr. 23, 2019) (complying with the CCPA means that businesses must update its policies and procedures as well as train all employees on handling data responsibly); *see also* Jonathan Pollard, *Tesla Sues Ex-Employee (Whistleblower?) for Theft of Trade Secrets*, POLLARD PLLC (June 21, 2018), https://www.pollardllc.com/tesla-trade-secrets-whistleblower/ (showing automakers face challenges with employees such as internal hacking and transfer of consumer data).

166 *See* Bruno, *supra* note 135 (training enables the employee to safeguard consumer information).

167 *See* Gabel, *supra* note 121 (explaining the remedies available to consumers upon a data breach).

168 *In re* Uber Techs., Docket No. C-4662, 2018, F.T.C., 1-2 (reasoning an actual breach must be proved when information is accessed without authorization); *see also* Norton, *supra* note 70 (stating PII is the most common form of data lost upon breach).

169 *See* Tung, *supra* note 115 (showing the hackers accessed the infotainment system via the internet by being near the vehicle).

170 *See* Cahen v Toyota, 717 Fed. App'x. 720 at 723-24 (showing mere vulnerability to a hack is not enough; however, alleging mere vulnerability to a hack and showing that a hack did occur will create liability on behalf of the manufacturer).

171 Tung, *supra* note 115.

data before a breach occurs.[172] VW and Audi would have been liable for a data breach if the hackers accessed consumer information from the vehicle infotainment systems because there were clear security flaws within the system.[173] To avoid liability, a business could implement a comprehensive privacy protocol, conduct privacy audits, retain records of bug bounty reports, and accurately represent its privacy measures.[174]

Further, the privacy protocol must parallel the actual safeguards in place.[175] A business could face liability if it attempts to mislead consumers by stating that it has great data protections in place when it does not actually have such protections.[176] For example, VW and Audi would be liable for a breach of its privacy statement if the privacy protocol stated consumers were protected from all outside intrusions and that the infotainment system was secure.[177]

Third, businesses must create a plan to stop the breach from happening once the business detects the breach.[178] Once breached,

---

172 *See Echavarria*, No. 5:18-cv-05982 at 4-6 (holding Uber liable for failure to adequately safeguard driver and user information and for lying about its policy and procedures).

173 *See* 2016 O.J. (L 119) 1 art. 32 (stating the business must implement "appropriate technical and organizational measures [ensuring] . . . security appropriate to the risk"); *see also Echavarria*, No. 5:18-cv-05982 at 4-6 (showing the business might be protected from liability if the business can prove that these protocols and safeguards were in place before the data breach).

174 After the Uber breach, the FTC made sure that Uber conducted third-party privacy audits. *See In re Uber Techs.*, Docket No. C-4662, at 2-7. A company must create a cybersecurity framework that identifies an organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities, and a safeguard that ensures that all critical infrastructure services are delivered and detects and identifies cybersecurity attacks. *See* Erika McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, DOC NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 1, 2-1 to 2-4, 10-11 (Apr. 2010) [hereinafter NIST].

175 *See In re Uber Techs.*, Docket No. C-4662, at 7 (mandating Uber create a privacy program that is reasonably designed to address privacy risks and protect data).

176 *Id.*

177 *See id.* (explaining the FTC investigated Uber for failing to adequately protect consumers after stating that consumers were protected); *see also* Tung, *supra* note 115 (explaining the VW and Audi hack).

178 *See* CAL. CIV. CODE § 1798.105(d)(2) (stating automakers "shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary . . . to maintain the

a business must create a comprehensive cybersecurity strategy that responds to the breach and recovers the stolen data.[179]

Assume that a hacker infiltrates a vehicle's infotainment system through a hole within the V2V network.[180] Once the hacker infiltrates the first vehicle's network, the hacker is now able to access a consumer's personal cell phone via V2I, enabling the hacker to gain access to the consumer's personal information.[181] In this case, the car company is likely liable because the data breach was possible because of the hole in the network.[182] To mitigate the liability, the company must create a security protocol which locks the hacker out of both the consumer's vehicle and the consumer's cell phone.[183]

Finally, a business must inform a consumer of a data breach within a reasonable time or within 72 hours of detection.[184] A

---

consumer's personal information in order to[] detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity").

179 *See Using NIST CSF to Overcome the 3 Hurdles of Security Maturity Reporting*, AXIO, https://axio.com/blog/using-nist-csf-to-overcome-the-3-hurdles-of-security-maturity-reporting/ (Dec. 18, 2018), (explaining a cybersecurity framework includes "implement[ing] appropriate activities to take action regarding a detected cybersecurity incident" and a recovery process that maintains resilience and restore[s] any impaired capabilities or services); *see also* NIST, *supra* note 174, at 5-1 to 5-3; *see also* Murphy, *supra* note 71.

180 *See generally* Tung, *supra* note 115 (examining a recent hack).

181 *Id.*

182 *See In re* Anthem, 162 F. Supp. 3d at 984-87 (explaining Anthem was liable for failing to take adequate and reasonable measures to ensure data systems protection).

183 *See* CAL. CIV. CODE §§ 1798.150 (West 2018) and 1798.81.5(d)(1)(A) (West 2016); *see also* Perez & Whittaker, *Everything You Need to Know About Facebook's Data Breach Affecting 50M Users*, TECHCRUNCH, https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/ (last visited Jan. 27, 2019) (showing upon breach, Facebook ensured the protection of the Facebook system as well as any linked accounts, such as Instagram and WhatsApp).

184 *See Driving Change*, KPMG LLP (2018), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwj3srapmb_lAhWJrFkKHVKTAAQQFjAAegQIARAC&url=https%3A%2F%2Fadvisory.kpmg.us%2Fcontent%2Fdam%2Fadvisory%2Fen%2Fpdfs%2Fdriving-change.pdf&usg=AOvVaw1CbQKP_lCyItedJ6qrEw5V (explaining under the GDPR, the company must notify consumers of a breach within 72 hours of detection and under the CCPA, the company must notify consumers without unreasonable delay).

business may avoid liability if it implements a privacy protocol program that informs consumers immediately of any significant data breach.[185] Unlike Uber's breach notification process, a car company should develop and implement strategies that stream line the notification process.[186] Similarly, businesses may avoid liability only if the consumers are reasonably informed of all aspects of the breach that are necessary to protect the consumer.[187] In addition to the business developing a system that automatically informs the consumers of a breach, the company must also train employees to adequately respond to consumer requests for information.[188]

iv. Data Privacy Liability

A manufacturer is likely liable for breaking consumer privacy when: (1) there is an invasion of privacy that led to the collection of "sensitive or individually identifiable" data; (2) it uses a person's information for advertising purposes without consumer consent; or (3) if it monitors and uses a person's data (i) without consent; (ii) outside of the necessary collection and use of the data; (iii) and invades a person's privacy.[189]

First, to be successful in a privacy claim, consumers must show an invasion of privacy that led to the collection of "sensitive or individually identifiable" data.[190] A company is likely not liable for a privacy breach if a hacker infiltrates a Jeep and takes control of

185 *See id.* (explaining the steps to remain compliant with the CCPA); *see also Echavarria*, No. 5:18-cv-05982 at 15-21.
186 *See In re* Uber Techs., Inc., Docket No. C-4662 at 1-5; *see also* NIST, *supra* note 176, at 3-5 (creating guidelines such as a company should create a system that automatically notifies impacted consumers of the breach via email or cellular message).
187 *See* CAL. CIV. CODE §§ 1798.81.5(d)(1)(A), 1798.150, 1798.155 (2016 & 2018) (operative January 1, 2020); *see also* 2016 O.J. (L 119) 1 art. 33; Lucas, *supra* note 69 (stating businesses must ensure risks are detected and consumers are informed).
188 *See* NIST, *supra* note 174, at 1-1; *see also* Perez, *supra* note 183 (showing that when hackers infiltrated and took control of a Jeep, the company quickly informed consumers and issued a recall to secure all holes within the network).
189 Cahen v Toyota, 717 Fed. App'x. 720 at 724.
190 *Id. But see* 18 U.S.C. § 2721 (1994) (explaining a business could protect itself from liability by proving that it used this information for legitimate business purposes).

the brakes, acceleration, or any other parts of the system.[191] However, a company is likely liable for a privacy breach if a hacker infiltrates a vehicle's infotainment center and collects a consumer's data relating to his or her use of the GPS, calling services, or text messages.[192]

Second, a manufacturer is liable if it uses a person's information without consent for advertising purposes.[193] This will impact auto manufacturers as infotainment technology advances and targeted advertisements are used and possibly shared among vehicles through V2V, V2I, and CVMA interactions.[194] A business could potentially avoid liability if its privacy policy fully informs the consumer of the data collection process.[195]

Third, a manufacturer is liable if it monitors and uses a person's data without consent, outside of the necessary collection and use of the data, and invades a person's privacy.[196] For example, an automaker could face liability if the company collects data relating to how a person utilizes their phone for online or application shopping.[197]

A company could argue that a consumer consented to the collection and use of this data because its privacy policy states that the company may collect all data that is reasonably necessary to

---

191 *See Cahen*, 717 Fed. App'x. 720 at 724 (merely alleging hack vulnerability is insufficient).
192 *See id.* at 724 (explaining a consumer must show data was collected and the data collected "was sensitive or individually identifiable"); *see also* Ganesan, *supra* note 13 (hacking a person's vehicle, if connected to a person's cell phone, sheds light on where the consumer goes in the car, when the person goes to the restroom, where the person goes to the doctor, or when the person is away from his or her desk at work).
193 Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 790 (N.D. Cal. 2011).
194 *See* Hawkins, *supra* note 47, at 2 (explaining how companies utilizes consumer's GPS and infotainment data to create targeted ads for companies like Starbucks or Dominos).
195 *See In re* Carrier IQ, 78 F. Supp. 3d 1051, 1091 (N.D. Cal 2015) (showing the consumer must consent to the use and sharing of the consumer's information for advertising purposes).
196 *See id*. at 1063; *see also id*. at 1076 (reasoning manufacturers may avoid liability if there were no "intercepted" communications) (citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002)).
197 *See id.* at 1063; *see also* Rupa Ganatra, *How LiketoKnow.it Is Driving Influencer Sales at Scale*, FORBES (Mar. 5, 2018, 1:08 pm), https://www.forbes.com/sites/rganatra/2018/03/05/liketoknow-it-driving-influencer-sales-at-scale/#48f44a7c2298 (showing LiketoKnow.it allows Instagram users to see and purchase clothes that Instagram influencers model on Instagram).

enhance the driver's experience in the vehicle.[198] However, it is unlikely that a court would find that the consumer knowingly consented to the collection of data related to their online shopping experience based on the company's very broad privacy policy.[199]

III. Automotive Compliance and Regulatory Schemes

GDPR and CCPA compliance is tedious but attainable through privacy protocols and safeguards that protect businesses from liability.[200] Specifically, business can enhance protections by implementing an auto-update system that deters potential hacks and glitches, by educating consumers, and by training employees.[201]

Compliance is attained by maintaining strict adherence to the privacy policy and safeguards. A business must be transparent regarding what data is collected and why, as well as how the data collection process works when gaining consumers' permission to collect.[202] This can be relayed to consumers when they purchase a vehicle, within the contract, and when consumers utilize any part of the vehicle that collects data.[203] Consumers should be notified

198 *See generally* Tesla Policy, *supra* note 19.
199 *See* CAL. CIV. CODE § 1798.185(a) (stating a company may utilize consumer data for business related purposes); *see also In re Carrier IQ*, 78 F. Supp. 3d at 1085 (reasoning providers may monitor communications for the purposes of ensuring that the providers appropriately route, terminate, and manage messages). *But see In re* Google, Inc., 58 F. Supp. 3d 968, 974-75 (N.D. Cal 2014) (reasoning a company is likely not liable, even if it strays from its privacy policy, when granting third-party access to data).
200 *See generally* Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1; *see generally* Cal. Civ. Code §§ 1798.100-98.
201 Gina Pingitore et al., *To Share or Not to Share,* DELOITTE: INSIGHTS (Sept. 5, 2017), https://www2.deloitte.com/insights/us/en/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html.
202 *See General Data Protection Regulation Guide*, *supra* note 32, at 5-6 (discussing how businesses should make information regarding data collection accessible to consumers).
203 Nancy L. Perkins et al., *California's New Privacy Statute: Is It a US GDPR?*, ARNOLD & PORTER LLP (Oct. 3, 2018), https://www.arnoldporter.com/en/perspectives/publications/2018/10/californias-new-privacy-statute (suggesting different methods

every time the data collection or use policy is altered, and consumers should opt-in yearly.[204]

Next, consumers must be informed of their right to access the collected data.[205] Businesses would benefit from creating either an in-car or telephone application that allows consumers to view collected data.[206] The application could connect the vehicle directly to a mobile device so the consumer can check a list of the data being used. To ensure security, the application need not show grand details of the used data, but should give the consumer a general understanding of the collected data. If consumers want access to a more detailed list, businesses should create protocols ensuring consumer access is efficient and effective.

Moreover, to give consumers a visual image of why the data is being collected, businesses could create a diagramed list that connects the collected data with the data collection purpose. Additionally, businesses must create a crisis-management infrastructure to alert consumers about security, privacy, fraud, and malfunction.[207] Finally, businesses should create ongoing employee trainings on GDPR and CCPA compliance because of technological privacy and protection growth.[208]

IV. CONCLUSION

---

businesses could incorporate to meet CCPA consent requirements).

204 *See* 2016 O.J. (L 119) 1, art. 13-14 (explaining when consumers should be provided information about data collection); *see also* CAL. CIV. CODE §§ 1798.110(c), 1798.100-1798.198; 1798.130(a)(5)(B), (C) (explaining compliance requirements for businesses collecting personal information).

205 *See* 2016 O.J. (L 119) 1, art. 12-23 (explaining consumers' rights to data collection information); *see also* CAL. CIV. CODE §§ 1798.100 (disclosing consumer rights regarding data collection); 1798.110(a)-(b) (discussing rights of consumers to request information from businesses); 1798.130 (explaining compliance requirements for businesses collecting personal information).

206 *See* Perkins, *supra* note 203 (explaining consumers have the right to know what personal information is collected, if that information is sold or disclosed, and the right to access).

207 *See* NIST, *supra* note 174, at 2-3 (showing protocols should be implemented guided by use limitation, security safeguards, openness, individual participation, and accountability).

208 CAL. CIV. CODE § 1798.130 (discussing businesses' compliance requirements regarding employee training); *see also Summary of California Consumer Privacy Act of 2018*, *supra* note 162 (requiring businesses to train employees).

The growth of automotive and data collecting technology is inevitable. Automakers and third-parties must plan ahead and ensure all data is protected before a breach or hack occurs. Moreover, these companies must preemptively develop and implement security measures that will not only protect the company from potential GDPR and CCPA fines, but also protect the company from potential lawsuits due to the mishandling of consumer data. Transparency is key for a company to protect the golden goose that is consumer data. This means that at the outset, consumers must know why their data is being tracked and used, and upon a data breach or hack, consumers must be informed of all of the necessary information that will ensure that the consumer's information is protected.