Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 29 | Issue 1 Article 3

12-13-2012

Turning a New LEAF: A Privacy Analysis of CARWINGS Electric Vehicle Data Collection and Transmission

Francesca Svarcas

TURNING A NEW LEAF: A PRIVACY ANALYSIS OF CARWINGS ELECTRIC VEHICLE DATA COLLECTION AND TRANSMISSION

Francesca Svarcas†

Abstract

Vehicles equipped with onboard telematics systems and wireless capabilities are redefining "mobile" computing. The resulting convenience and access to data raise privacy concerns with respect to consumers' geolocations and driving behaviors. This article describes the types of data collected and transmitted by technologies that are currently being used in or in connection with electric vehicles. While the following descriptions and analyses of event data recorders, GPS, RSS feeds, vehicle telematics, and wireless communications are specific to the 2011 Nissan LEAF, the application and use of these devices are relevant to what may become industry standards. Nissan, for example, provides new LEAF owners with a subscription to CARWINGS telematics services. In view of the Federal Trade Commission's March 2012 Final Report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers," the CARWINGS telematics services subscription agreement falls short in terms of disclosing essential information about the vehicle's ability to collect and transmit data and how these capabilities impact individuals' privacy. Meanwhile, common law constitutional privacy protections exist, but remain limited in the context of automotive vehicles and leave unanswered questions regarding related methods of electronic surveillance.

---

† Francesca Svarcas is an Adjunct Instructor for California State University East Bay's Paralegal Studies Program. She has practiced as a litigation associate at Burnham Brown in the areas of toxic tort defense and insurance coverage. Mrs. Svarcas is currently earning her LL.M. degree in Intellectual Property Law at Santa Clara University School of Law where she previously obtained her J.D. She holds a B.A., *cum laude*, from Franklin & Marshall College. Mrs. Svarcas is grateful for the encouragement and mentorship of Professor Dorothy J. Glancy throughout the process of writing this article and for Professor Glancy's ongoing commitment to keeping alive a discussion of consumer and transportation privacy interests.

TABLE OF CONTENTS

I. INTRODUCING THE LEAF

In December of 2010, foreign vehicle manufacturer, Nissan, released the LEAF, an all-electric vehicle (EV) equipped with a toy box of technology features including a rear-view camera, Bluetooth hands-free telephone system, MP3 audio system, XM satellite radio, USB connection ports for iPod, and steering wheel-mounted voice controls.[1] The ultimate convenience promoted by Nissan, however, is the vehicle's lithium-ion batteries: the owner will never need to set foot in a gas station for the purpose of fueling the automobile.[2] Neither will the owner need to stop and ask for directions. This is because the LEAF embraces technological advances in telematics—a two-way telecommunications system that is built into the vehicle[3]—and GPS navigation. As with many innovative products, consumers must weigh the cost of convenience against how use of the technology impacts individuals' privacy, particularly in terms of how their personal data is collected and used by others. Justice Alito, in penning the recent United States Supreme Court concurring opinion in *United States v. Jones*,[4] recognized the following trends: "New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[5]

Fortunately, this near giving up of one's privacy rights does not have to happen so quickly or consensually. Justice Alito speaks in terms of "many people," not "all people." Therefore, it is the hope of at least some privacy-minded consumers that constitutional privacy and other legal protections still apply. This article, for example, takes a careful look at privacy considerations associated with the technologies and conveniences offered by the 2011 Nissan LEAF. Specifically, this article explores the vehicle's CARWINGS telematics system, global positioning system (GPS), event data

---

1. NISSAN USA, http://www.nissanusa.com/leaf-electric-car/versions-specifications?next=ev_micro.section_nav (last visited June 29, 2012).

2. *See id.* (claiming LEAF's fuel efficiency of "up to 100 miles per charge").

3. Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 302 (2004).

4. 132 S. Ct. 945 (2012).

5. *Id.* at 962 (Alito, J., concurring).

recorder (EDR), and really simple syndication (RSS) capabilities. An analysis of Nissan's Telematics Services Subscription Agreement follows with respect to how consumer data is collected and transmitted via EV technologies.

II. EV TECHNOLOGY

Today's vehicles monitor, collect, and store data in a variety of ways, one of them being through EDR technology. Like most twenty-first century vehicles, the LEAF is equipped with an EDR, which preserves a record of data being monitored in relation to air bag deployment.[6] Typically, an EDR will store data for five to twenty seconds, and can be used after a crash to understand how the air bags worked as well as provide information about the accident that triggered air bag deployment.[7] For example, the LEAF records data such as "the direction from which [the vehicle] was hit and which air bags have deployed."[8] EDRs also record a snapshot of data "when a vehicle senses a potential collision," thereby temporarily storing information about the driver's behavior in instances where an accident has not occurred.[9]

Additionally, the vehicle includes a preinstalled GPS navigational system. GPS is a "satellite-based technology that reveals information about the location, speed, and direction of a targeted subject."[10] Similar to portable GPS devices, the owner can save locations including his or her home address, create an address book and plan trip routes.[11] EDRs are not typically connected to GPS systems, and there is no indication that these two devices are connected in the LEAF. However, the vehicle is disclosed as being

---

6. 2011 LEAF OWNER'S MANUAL REVISED 9-18 (2011), *available at* http://www.nissan-techinfo.com/refgh0v/og/leaf/2011-nissan-leaf.pdf.

7. Andrew Askland, *The Double Edged Sword That Is the Event Data Recorder* 1-2 (bepress Legal Series, Working Paper No. 1255, 2006), *available at* http://law.bepress.com/expresso/eps/1255.

8. Nissan LEAF Telematics Subscription Services Agreement ¶ 11.2 [hereinafter CARWINGS Agreement] (on file with author).

9. Dorothy J. Glancy, *Retrieving Black Box Evidence from Vehicles: Uses and Abuses of Vehicle Data Recorder Evidence in Criminal Trials*, THE CHAMPION, May 2009, at 12, *available at* http://www.nacdl.org/champion.aspx?id=14699.

10. Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 414 (2007).

11. *See* 2011 LEAF NAVIGATION SYSTEM OWNER'S MANUAL 1-7, 1-12 (2011), *available at* http://www.nissan-techinfo.com/refgh0v/og/leaf/2011-Nissan-LEAF-Navi.pdf.

equipped with additional undefined "electronic modules" that monitor and record data involving the vehicle's motor, batteries, brakes and electrical system.[12] Even though the vehicle owner's manual does not provide further descriptive information about this technology, the "electronic modules" appear to be distinct from the EDRs, and evidently capture behavioral data such as the driving habit and style of the individual operating the vehicle.[13]

A veritable smartphone on wheels, the LEAF also has RSS subscription capabilities, accessible as information feeds through CARWINGS.[14] RSS is a syndicating news format, the acronym for which represents multiple titles such as Really Simple Syndication, Rich Site Summary and RDF Site Summary.[15] Described as a "simple XML-based system," CARWINGS allows users to utilize RSS to subscribe to news feeds that can then be viewed online, through web pages and browsers.[16] There is usually an accompanying RSS icon that can be found either on the page or in the URL window, indicating that the web page can be syndicated and that the feed can be added as a "live bookmark."[17]

Data from the above technologies can be transmitted from the user to Nissan through the vehicle's telematics. The telematics system is a combination of software and hardware installed in the vehicle that "sends and receives information via wireless and landline communications networks" as well as GPS signals.[18] Specifically, Nissan provides LEAF owners with CARWINGS telematics services pursuant to a subscription services agreement. The telematics system has multiple components from which data can be transferred or accessed, including the vehicle's cellular modem, the CARWINGS web-based interface, and a data center operated by Airbiquity.[19]

---

12. 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-16.

13. *See id.*

14. Password protected CARWINGS website, accessible to LEAF owners through Nissan's Online Portal, https://www.nissanusa.com/owners/login (after login, follow the "View LEAF Status," then "launch CARWINGS," and then "All Info. Feeds" hyperlinks) (last visited Oct. 30, 2012). *See also* 2011 LEAF NAVIGATION SYSTEM OWNER'S MANUAL, *supra* note 11, at 5-7, 5-9 to -10.

15. Hugh Calkins, *Something About Technology: Really Simple Syndication*, 21 ME. B.J. 190, 190 (2006).

16. *Id.*

17. *Id.* at 191.

18. CARWINGS Agreement, *supra* note 8, ¶ 6.

19. *Carwings Protocol*, MYNISSANLEAF WIKI,

Additionally, there is a proxy endpoint (or destination) associated with LEAF owners who connect their vehicles to their smart phones using iOS and Android applications.[20]

New LEAF owners are already noticing different types of information being collected about them and are piecing this together with the vehicle's capacity to transmit the data to others. One owner, for example, posted a video online in June of 2011 about his locational data being sent to RSS providers.[21] As the GPS tracked the driver's location, speed, and direction, that data was then wirelessly transmitted to RSS providers. Interestingly, the article that features the video contains the following statement from Nissan, purportedly given in response to the article:

> Owners have to opt in or agree to share their data every time they sign in. If they don't, then they pass on the benefit as well. They will however, lose any remote control or data logging capability but the choice is in the hand of the driver every time.[22]

This article questions the validity of Nissan's "opt-in" method by evaluating the CARWINGS telematics subscription services agreement. Also, since the RSS testing on the LEAF described in the video occurred more than a year ago, this article provides results for a more recent examination of whether location information can be leaked through CARWINGS in Part IV.G below.[23]

The LEAF's ability to send and receive wireless and cellular transmissions, paired with the types of data that the vehicle is able to collect, raises serious privacy concerns with respect to both personal information privacy and autonomy privacy. Personal information privacy, also known as access-control privacy, includes data about a person such as their name, address, Social Security number (SSN),

---

http://www.mynissanleaf.com/wiki/index.php?title=Carwings_protocol (last modified Aug. 20, 2011).

20. *Id.*

21. Edward Niedermeyer, *Nissan Leaf Owner Exposes CarWings Privacy Issue*, THE TRUTH ABOUT CARS (June 13, 2011), http://www.thetruthaboutcars.com/2011/06/nissan-leaf-owner-exposes-carwings-privacy-issue/.

22. *Id.*

23. The 2011 LEAF tested for purposes of this article belongs to the author who purchased the vehicle in June 2011 and began her research for this article in January 2012. Since then the vehicle has undergone software updates at a local Nissan dealership, the specifics of which are unknown to the author.

likes and dislikes.[24] The mere transfer of these types of data to others who are not entitled to the information can impinge upon an individual's privacy rights. As discussed later in the article, Nissan does at a minimum encrypt sensitive information, which it defines as location, credit card information, usernames, and passwords.[25]

Autonomy privacy involves a person's choice in making decisions and engaging in conduct without interference from intrusion by the government or other nongovernmental entities.[26] Once an individual knows or suspects that he or she is being monitored by enhanced surveillance techniques, that person may even go so far as to modify his or her behavior.[27] While an individual may already want to abide by the speed limit for purposes of obeying the law, that person may become even more likely not to speed out of a sense of paranoia, knowing that someone else is privy to that data. "We behave differently when we know that we are being observed . . . ."[28] This behavioral reaction essentially strips the individual of his or her freedom of choice. Moreover, knowing or suspecting that third parties have a record of the driver's location data, the individual may think twice about that trip to the mistress's home or a destination that would implicate one's freedom of association.

III. CARWINGS

Nissan provides its customers with complimentary CARWINGS telematics services for the first three years of LEAF ownership.[29] This system allows a user to monitor the vehicle's charge settings, climate control settings, and navigation system updates from the user's smartphone or computer.[30] To use CARWINGS, the owner enters into a contract with Nissan entitled "Telematics Subscription Services Agreement" (also referred to as "CARWINGS Agreement"). This

24. *See* Glancy, *supra* note 3, at 370. *See also* DECKLE MCLEAN, PRIVACY AND ITS INVASION 121-22 (1995).

25. CARWINGS Agreement, *supra* note 8, ¶ 11.4.

26. Glancy, *supra* note 3, at 321-22.

27. *See* DAVID D. FRIEDMAN, FUTURE IMPERFECT: TECHNOLOGY AND FREEDOM IN AN UNCERTAIN WORLD 66-82 (2008).

28. Askland, *supra* note 7, at 13.

29. CARWINGS Agreement, *supra* note 8, ¶ 1.

30. *See CARWINGS*, NISSAN USA, http://www.nissanusa.com/leaf-electric-car/home-charging?next=ev_micro.key_features.charging_ah.link#_carwings-section (last visited June 30, 2012).

happens during an online registration process where the customer is asked by Nissan to provide the vehicle's identification number (VIN) and accept the Nissan CARWINGS "Terms of Use."[31]

A. Limited Availability of the CARWINGS Agreement

After the customer accepts the terms of use, the CARWINGS Agreement appears to take flight. The LEAF Owner's Manual states that the CARWINGS Agreement can be accessed on the Nissan Owner's Portal, a website where users can view their Nissan account information and connect to CARWINGS services.[32] Unfortunately, this is not the case. The only option available to the customer from within the Owner's Portal is to send Nissan a message through a customer service request form.[33] In response to such a request, Nissan EV Customer Support has confirmed that once the terms of the CARWINGS Agreement are accepted online, they are "no longer able to be seen."[34] Nissan EV Customer Support then promises that it will contact the customer once a copy is available.[35]

As a result of amendments to the Federal Trade Commission Act (FTCA),[36] there are Federal Trade Commission (FTC) requirements specific to online privacy policies.[37] Unlike OnStar and Mercedes-Benz who both provide the terms and conditions of their telematics services agreements as well as separate stand-alone privacy policies specific to their telematics services, Nissan provides only the telematics services subscription agreement.[38] There is no separate

---

31. *Using Nissan CARWINGS*, NISSAN GREAT BRITAIN, http://www.nissan.co.uk/GB/en/YouPlus/carwings.html (last visited Oct. 8, 2012).

32. 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-17.

33. Password protected Nissan's Online Portal, *supra* note 14 (last visited June 22, 2012) (containing a hyperlink "Contact Nissan" that leads to http://www.nissanusa.com/apps/contactus).

34. E-mail from Nissan EV Customer Support to author (Jan. 27, 2012, 13:18 PST) (on file with author).

35. *Id.*

36. *See* 15 U.S.C. §§ 41-58 (2011).

37. *See* In the Matter of Geocities, Inc., File No. 9823015, 1998 WL 473217 (F.T.C.) (1998) [hereinafter Geocities], *available at* http://www.ftc.gov/os/1998/08/geo-ord.htm (agreement containing consent order). *See also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 57, 59 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC REPORT].

38. *Terms and Conditions of Your OnStar Service*, ONSTAR (Aug. 2010), *available at* http://www.onstar.com/web/portal/termsconditions; *Our Privacy Practices*, ONSTAR (Jan. 1,

CARWINGS or Nissan telematics privacy policy.[39] In terms of what consumer data is collected by Nissan through CARWINGS, and how that data is used, the CARWINGS Agreement contains privacy disclosures for which clear and prominent notice to the user is required "in connection with the online collection of personal identifying information,"[40] as well as a hyperlink to the privacy notice.[41] Nissan CARWINGS fails to satisfy both requirements. Consequently, the consumer is left with the uncomfortable burden of following up with Nissan to obtain a copy of an agreement that should be readily accessible.[42]

Once obtained, the customer will notice that the CARWINGS Agreement is actually entitled "Nissan LEAF Telematics Subscription Services Agreement."[43] Briefly, the terms generally reflect that the consumer and Nissan enter into a three year agreement, effective on the first purchase of the LEAF from Nissan, the cost of which is included as part of the vehicle purchase price.[44] Once the three-year subscription expires, Nissan and the customer may enter into a separate agreement for additional services at the market rate at that time.[45] Although CARWINGS does not appear to be advertising its

---

2011), *available at* http://www.onstar.com/web/portal/privacy; *Mercedes-Benz mbrace Terms of Service*, MERCEDES-BENZ (May 3, 2012), http://www.mbusa.com/vcm/MB/DigitalAssets/pdfmb/brochures/mbrace-subscriber.pdf; *Mercedes-Benz—HUGHES Telematics Privacy Policy—mbrace Service*, MERCEDES-BENZ (Nov. 16, 2009), http://mbrace.mbusa.com/legal-page.htm.

39. Unlike the OnStar and Mercedes-Benz telematics services agreements, the CARWINGS Agreement does not reference a separate telematics privacy policy. *See* CARWINGS Agreement, *supra* note 8. Neither do Nissan's owner's manuals. *See* 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6; s*ee also* 2011 LEAF NAVIGATION SYSTEM OWNER'S MANUAL, *supra* note 11. Paragraph 8 of the CARWINGS Agreement suggests that Nissan may provide online access to user data and that the website will be governed by the privacy policy of that website. *See* CARWINGS Agreement, *supra* note 8, ¶ 8. The only link to a privacy policy from the Nissan Owner's Portal where the user accesses CARWINGS is to Nissan's general privacy policy regarding website use. *See Privacy Policy*, NISSAN USA, http://www.nissanusa.com/global/privacy.html (last visited May 3, 2012). The general privacy policy appears to deal only with information Nissan collects on its website. *Id.* It is unclear whether use of the vehicle's telematics system constitutes use of the website.

40. Geocities, *supra* note 37, at *3. *See also* FTC REPORT, *supra* note 37, at 58-59.

41. Geocities, *supra* note 37, at *4; FTC REPORT, *supra* note 37, at 69-70.

42. E-mail from author to Nissan EV Customer Support (Jan. 23, 2012, 18:41 PST) (on file with author); E-mail from author to Nissan EV Customer Support (Feb. 14, 2012, 13:28 PST) (on file with author).

43. CARWINGS Agreement, *supra* note 8.

44. *Id.* ¶¶ 1, 3.

45. *Id.* ¶ 3.

current and future rates for its telematics services, it is likely that pricing will be similar to comparable services such as OnStar plans that range from $199 to $299 per year.[46]

B. CARWINGS Consent Pop-Up Screen: An Opt-In Copout?

Instead of providing a link to the full CARWINGS Agreement that a customer could revisit and download, Nissan reattempts to gain the driver's permission to transmit and use vehicle data via a pop-up message that appears on the display screen each and every time the vehicle is started. Even after accepting the CARWINGS Agreement, an owner (or guest driver) of the LEAF must repeatedly either accept or decline his or her consent to CARWINGS services and other wirelessly transmitted recorded vehicle data. The pop-up consent statement provides:

> Your vehicle wirelessly transmits recorded vehicle data to Nissan per subscription agreement for various purposes, including CARWINGS services, product evaluation, research and development. By touching OK, you consent to the transmission and use of your vehicle data. See Owner's Manual or Nissan website for terms and details.
>
> Touch OK to accept.
> [OK] [Decline][47]

As discussed above, the Owner's Manual and Nissan website are inadequate in providing "terms and details" because the CARWINGS Agreement is not available or accessible from the Owner's Portal after the customer accepts the terms of use. Presumably, a customer wouldn't even see this screen unless he or she had already registered the vehicle for CARWINGS services. Therefore, the pop-up screen's references to the Owner's Manual and Nissan website are circular—each source points to another for purposes of reviewing an agreement that Nissan admits is no longer available for viewing.[48] Nissan even forewarns the owner of the ongoing pop-up screen in the Telematics Subscription Services Agreement in all caps:

---

46. *See Explore OnStar Plans & Pricing*, ONSTAR, https://www.onstar.com/web/portal/planspricing (last visited Sept. 23, 2012).

47. Photograph: 2011 Nissan LEAF Navigation Control Screen (Francesca Svarcas, June 22, 2012) (on file with author). *See also* 2011 LEAF NAVIGATION SYSTEM OWNER'S MANUAL, *supra* note 11, at 1-5; 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-17.

48. E-mail from Nissan EV Customer Support to author, *supra* note 34.

> In addition, you shall be required to acknowledge, via a pop-up consent statement presented on the navigation screen of your Nisan LEAF, that as part of the telematics services your Nissan LEAF transmits recorded vehicle data to Nissan for various purposes, including without limitation CARWINGS services, product evaluation, and research and development. If you click on the "Decline" button, your use of the telematics services will be very limited.[49]

IV. THE FTC'S POSITION ON PRIVACY DISCLOSURES AND PRACTICES

The FTC protects consumers' privacy by enforcing Section 5(a) of the FTCA, codified in 15 U.S.C. § 45(a), in cases alleging "unfair or deceptive acts or practices."[50] The FTC's authority under the FTCA extends to its recommended guidelines regarding privacy policies. In the Commission's March 2012 Final Report entitled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," the FTC calls upon Congress to consider the enactment of privacy legislation that would address companies' "unauthorized or improper use and sharing" of consumers' personal information.[51] Meanwhile, companies that collect and share sensitive consumer data must adhere to the privacy framework outlined in the FTC's report.[52] Where the framework exceeds, but does not conflict with existing statutory requirements, the FTC instructs companies regulated under those statutes to view the framework as "best practices to promote consumer privacy."[53] Additionally, companies that collect limited amounts of nonsensitive consumer data are not exempt from compliance if they share the data with third parties.[54] The FTC cites SSNs, as well as geolocation, financial, health and children's

---

49. CARWINGS Agreement, *supra* note 8, para. 4 (original all caps).

50. *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief at 2, FTC v. Hope for Car Owners, LLC, No. 2:12-CV-00778 (E.D. Cal. Mar. 27, 2012), *available at* http://www.ftc.gov/os/caselist/1223021/120404hopecmpt.pdf; Andrew Serwin, The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices, Version 2.0 2, 7 (Dec. 31, 2010) (unpublished manuscript), *available at* http://ssrn.com/abstract=1733217.

51. FTC REPORT, *supra* note 37, at 12-13.

52. *See id.* at 13, 15-16, 22.

53. *Id.* at 16.

54. *Id.* at 16, 22.

information as examples of sensitive data.[55]

The FTC's March 2012 framework is instructive as to essential disclosures and privacy practices regarding the following categories that would also apply to the CARWINGS Agreement: (1) consumer's consent and choice,[56] (2) the types of data collected, (3) how data is collected, (4) how the information is used, (5) disclosures of data to others,[57] (6) customer's access,[58] (7) data security,[59] and (8) other entities' collection of data.[60]

A. Validity of CARWINGS Consent Given by the Customer

In enforcing the FTCA, the Commission has interpreted Section 5(a) to require companies to obtain their customers' consent when collecting personally identifiable information.[61] Further, companies should obtain affirmative express consent,[62] in the form of an opt-in, from customers before collecting sensitive information such as geolocation data.[63] Additionally, the FTC reaffirms in the Final Report its longstanding requirement for companies to obtain express

---

55. *Id.* at 15.

56. *Id.* at 48, 57-60.

57. *See id.* at 36, 39 & n.184, 51 & nn.243-44, 62 n.305. *See also* Geocities, *supra* note 37.

58. FTC REPORT, *supra* note 37, at 64, 71.

59. *Id.* at 24, 30.

60. *See id.* at 39, 51 & n.244, 62 n.305.

61. Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61, 117 (2011).

62. The FTC in its 2012 Report mentions the following:

> Companies may seek "'affirmative express consent" from consumers by presenting them with a clear and prominent disclosure, followed by the ability to opt in to the practice being described. Thus, for example, requiring the consumer to scroll through a ten-page disclosure and click on an "I accept" button would not constitute affirmative express consent.

FTC REPORT, *supra* note 37, at 57, n.274. A definition of "affirmative express consent" is noticeably absent. The Privacy Rights Clearinghouse has commented on the FTC's failure to define "express affirmative consent" and hoped that it would do so in the In the Matter of Google, Inc. consent order. *See* Comments of Privacy Rights Clearinghouse before the Federal Trade Commission, In the Matter of Google, Inc., File No. 1023136 (May 2, 2011), *available at* https://www.privacyrights.org/google-buzz-proposed-consent-order-comments. It appears that the FTC has yet to provide such a definition. *See* In the Matter of Google, Inc., File No. 1023136, Docket No. C-4336, 2011 WL 5089551 (F.T.C.), at 12-13 (Oct. 13, 2011), *available at* http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.

63. FTC REPORT, *supra* note 37, at 59-60.

affirmative consent before using data in ways that are materially different from that claimed at the time collected.[64] The consent requirements function in conjunction with the framework's requests that companies provide "specific information and choice at a time and in a context that is meaningful to consumers" and craft privacy statements that consumers can easily understand and compare with other companies' data practices.[65]

At first glance, the CARWINGS Agreement—when it is made available—appears to be more or less in compliance in terms of providing information directed towards the various disclosure categories outlined above in order for the LEAF owner to consent to and accept the agreement. The first question is whether or not Nissan's potential noncompliance with the FTC requirements regarding the accessibility of the full agreement is enough to invalidate consent. The pop-up consent screen, alone, is useless without sufficient opportunity to review the CARWINGS Agreement. In some ways, the consent issues are similar to those that have been encountered in dealing with shrink-wrap and end-user license agreements (EULAs).[66] The customer must either agree to CARWINGS terms and conditions, including extensive limitations on and releases of Nissan's liability, or not benefit from the full service of the telematics system.[67]

Secondly, it is highly unlikely that a consumer purchasing the LEAF in 2011 would have understood from the terms of the Agreement that geolocation data could have been transmitted through RSS feeds the LEAF owner subscribed to through CARWINGS. In the context of transparency, the FTC's final principle regarding privacy notices is that the "notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[68] If not stated in the CARWINGS Agreement

64. *Id.* at 57-58, 60.

65. *Id.* at 58. Of note, the FTC REPORT addresses language for privacy policies, *id.*, which are statements of fact regarding a company's privacy practices whereas the CARWINGS Agreement is a contract containing privacy disclosures that are binding terms.

66. *See, e.g.*, Mo Zhang, *Contractual Choice of Law in Contracts of Adhesion and Party Autonomy*, 41 AKRON L. REV. 123, 126 (2008) (discussing the controversy over shrink-wrap agreements as contracts of adhesion).

67. Further information regarding releases of liability found in the CARWINGS Agreement appears *infra* Part IV.G entitled "Other Entities' Collection of Data Glossed Over by Broad Releases of Liability."

68. FTC REPORT, *supra* note 37, at 64.

upfront, this information should prominently appear in a brief privacy notice on the CARWINGS website when a user attempts to subscribe to an RSS feed. This would clearly be an appropriate time to provide the notice and would also establish a context that is meaningful to the consumer in terms of making a decision regarding consent.[69]

B. Types of Data Collected

"Because electric vehicles are designed as rolling computers, they are well suited to track data . . . ."[70] The most practical, and perhaps most uniquely identifiable, piece of information that Nissan collects is the VIN.[71] In addition, Nissan collects driving behavior data, location data, information regarding electric vehicle functions, data regarding the owner's use of the telematics services, and "other spot data."[72] Some data is stored while "other data concerning [the] vehicle's operation and performance is wirelessly transmitted by cellular connection through the vehicle onboard telematics system upon vehicle start-up or at other intervals to NISSAN."[73] Nissan discloses most of the information regarding the types of data collected in the CARWINGS Agreement. The LEAF Owner's Manual supplements information not found in the Agreement.

Since some of the data moves online via the CARWINGS website state regulations such as California's Online Privacy Protection Act (OPPA)[74] apply, and as a result add protections and

---

69. *See id.* at 58. It is interesting to consider whether Nissan knew about the RSS feeds leaking geolocation data before the June 2011 CARWINGS video was posted. *See supra* note 21. If this was a result that Nissan had not anticipated, then it is worth considering what other potential privacy breaches may exist.

70. Nathalie Weinstein, *Electric Vehicles the Guinea Pigs for Mileage Fee*, DAILY J. COM. (Oct. 13, 2010), *available at* http://djcoregon.com/wp-content/plugins/tdc-sociable-toolbar/wp-print.php?p=60468 (paraphrasing sustainable transportation program manager for the Oregon Transportation Research and Education Consortium John MacArthur). Electric vehicles are being targeted for use in tracking data such as the number of miles traveled within the state of Oregon for a mileage-based fee project. *Id.* It is reported that initially, in 2006, there was some resistance because of drivers' "privacy concerns about aftermarket GPS devices being installed in their vehicles." *Id*. Vehicles are now more commonly manufactured and sold equipped with GPS devices already installed. *Id.*

71. CARWINGS Agreement, *supra* note 8, ¶ 11.2. *See also infra* Part IV.F entitled "Constitutional Considerations Regarding CARWINGS Collection and Use of EV Data" (discussing VIN as a unique identifier).

72. CARWINGS Agreement, *supra* note 8, ¶ 11.2.

73. 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-16.

74. Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575-22579

requirements similar to those recommended by the FTC. These requirements include the conspicuous posting of a privacy policy where a commercial website or online service collects personally identifiable information "through the Internet about individual consumers residing in California" who either use or visit the website.[75] The privacy policy must "[i]dentify the categories of personally identifiable information" collected.[76] The statute includes the following as some of the types of data in its definition of "personally identifiable information": a first and last name, address, e-mail address, telephone number, SSN, "any other identifier that permits the physical or online contacting of a specific individual" and "[i]nformation concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier."[77]

1. Driving Behavior Data

Nissan equipped the LEAF with EDRs as well as "electronic modules that monitor, control and record data concerning various vehicle systems, including the motor, batteries, braking and electrical systems."[78] Therefore, in addition to capturing EDR data regarding accidents involving the vehicle,[79] the LEAF more generally tracks information such as idling, braking, and acceleration that paints a picture of the owner's driving habit and style.[80] Similarly, Nissan keeps track of the owner's use of the vehicle's air conditioner and headlights.[81] There is a small solar panel on the roof of the vehicle from which energy is used to charge accessory batteries.[82] Since the air conditioner and headlights run off of the accessory batteries,[83] so as to not drain the batteries intended to propel the vehicle, there is a logical connection here in terms of data being collected to monitor the

(West 2008).

75. CAL. BUS. & PROF. CODE § 22575(a) (West 2008).

76. *Id.* § 22575(b).

77. *Id.* § 22577(a).

78. 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-16.

79. CARWINGS Agreement, *supra* note 8, ¶ 11.2.

80. *See* 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-16. *See also* CARWINGS Agreement, *supra* note 8, ¶ 11.2.

81. *See* 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-16.

82. *Id.* at EV-30.

83. *See id.* at EV-2.

vehicle's performance.

The information collected presumably becomes important from a marketing standpoint for the purposes of studying optimal use of the vehicle's battery life and regenerative braking system. The driving data would likewise be useful for products liability purposes, including the identification of a potential vehicle equipment defect or malfunction, an understanding of whether the driver maneuvered the vehicle in a way that contributed or led to an accident and the discovery of facts in support of other theories of causation.

2. Location Data

The LEAF can also record location and trip data via the GPS navigation system.[84] The types of information tracked and or recorded include the car's speed, distance traveled, and precise location.[85] The most accessible source for finding trip data is the vehicle itself. The GPS navigation screen includes an address book that the owner can configure and a history of the owner's recent destinations,[86] as well as incoming and outgoing telephone calls made using Bluetooth connections between the vehicle and a cell phone.[87] On the control screen the vehicle owner can also review and store locations, routes, previous destinations, and areas to avoid.[88] Since the navigation and other menu settings on the vehicle's control panel are not password protected, a thief or other unauthorized driver of the vehicle could easily obtain this data. This is particularly dangerous where the owner has entered his or her home address as a destination point.

3. EV Functions and Use of Telematics Services

Nissan also keeps track of the electric vehicle's functions and its customers' use of the telematics services. Among the various categories of data included here are battery use management, battery charging history, battery deterioration, electrical system functions and software version information.[89] The vehicle owner's use of the telematics services refers to the use of CARWINGS and its

84. *See id.* at 9-16.

85. *Id.*

86. 2011 LEAF NAVIGATION SYSTEM OWNER'S MANUAL, *supra* note 11, at 3-27.

87. *Id.* at 7-8.

88. *Id.* at 3-27, 3-55 to -59.

89. CARWINGS Agreement, *supra* note 8, ¶ 11.2.

corresponding website and smartphone application.[90] Finally, Nissan discloses the collection of "other spot data" used to "assist in identifying and analyzing the performance" of the vehicle.[91] It is unclear as to exactly what Nissan means to include in this final catchall category of spot data. At first glance, it appears to be oriented towards the actual vehicle technology, but as seen above, this could include many things.

C. How Data is Collected

The CARWINGS Agreement clearly, but broadly, identifies multiple methods by which Nissan collects data. The first source of data is information that the customer provides to the Nissan dealer where the vehicle is purchased.[92] Nissan continues to collect information from its customers via communications such as telephone calls and emails between the customer and Nissan, as well as through the customer's use of the telematics system.[93] Other sources of information include data provided by Nissan's wireless carrier, AT&T,[94] and information collected by the vehicle itself.[95]

D. How Information is Used

Nissan provides multiple altruistic reasons for using the data collected. Among these are desires to troubleshoot, maintain, and improve vehicle performance, evaluate and improve telematics services, and prevent fraud or misuse of the telematics services.[96] The CARWINGS agreement also cites a couple of marketing motives such as performing market research and offering new or additional products or telematics services.[97] The Owner's Manual likewise lists a number of consumer-friendly purposes for the data collection such as

---

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.*; Photograph: 2011 Nissan LEAF Settings Control Screen, Data Communications (Francesca Svarcas, June 22, 2012) (on file with author); *AT&T 3G Will Power the New Nissan LEAF, From In-Car Media to Remote Battery Level Monitoring*, REMOVE THE LABELS (Aug. 1, 2010), http://www.removethelabels.com/2010/08/01/att-3g-will-power-the-new-nissan-leaf-from-in-car-media-to-remote-battery-level-monitoring/.

95. CARWINGS Agreement, *supra* note 8, ¶ 11.2.

96. *Id.* ¶ 11.3.

97. *Id.*

troubleshooting and improving vehicle performance.[98] However, one can imagine additional uses and misuses for this information, especially by the "third party service providers such as cellular, information systems and data management providers" identified by Nissan as parties with whom Nissan may be sharing vehicle data.[99]

A more well-known use among LEAF owners is that Nissan combines the data and compares it with data gathered from other LEAF owners to determine aggregate product usage.[100] Despite denials to the contrary, Nissan does this through what appears to be friendly competition between vehicle owners by giving each owner an energy economy rating of silver, gold or platinum to indicate how well they are driving.[101] The driver also has an opportunity to grow virtual trees, called Eco Trees, while the car is in operation.[102] The trees are intended to show how much the driver is contributing to the environment by driving an electric car in lieu of a gas powered vehicle. The driver can then log into the CARWINGS website to compare his or her tree-growing accomplishments to others' and admire the virtual forest generated by the reigning first place winner. What the CARWINGS Agreement does not say is if the above method of internal data aggregation is paralleled by external data aggregation efforts between Nissan and third parties with access to the customers' data. Aggregate information is defined in terms of wireless telecommunications usage in the Telecommunications Act of 1996[103] as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[104] This may very well be happening with electric vehicle data, after Nissan shares the vehicle data with third parties, although it is not specifically disclosed as such in the CARWINGS Agreement.

---

98. 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-16.

99. *Id.*

100. CARWINGS Agreement, *supra* note 8, ¶ 11.3.

101. Password protected CARWINGS website, *supra* note 14 (Nissan includes the following disclaimer on the CARWINGS website regarding energy economy rankings: "Rankings are only for informational use and is [sic] not intended to promote a competition. Always obey traffic laws and follow instructions in your Nissan LEAF owner's manual.").

102. *Id.*

103. Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

104. 47 U.S.C. § 222(h)(2) (2008).

E. Disclosure of Information to Others

Nissan discloses that it will, and that the owner agrees that it can, make use of any information collected and share that information with service providers, roadside assistance providers, emergency service providers or "others, as needed."[105] "Service provider," as defined early on in the agreement, includes

> any person, company, subsidiaries or affiliates or entity who provides any service, equipment, or facilities in connection with Telematics Services, including, but not limited to, wireless service providers, suppliers, licensors, public safety answering points, emergency responders and Service Providers (such as police, fire and ambulance), towing companies, and Nissan LEAF distributors and dealers.[106]

From here, it is the customer's best guess as to which of these third parties are receiving what categories of data collected by Nissan, and for what purpose.

F. Owner's Rights in and Access to CARWINGS Driving Data

The customer owns all rights, title and interest in all data collected through the vehicle's telematics.[107] However, by accepting the CARWINGS Agreement, the customer grants Nissan a "worldwide, royalty-free, fully paid, transferable, assignable, sublicensable . . . [and] perpetual license to collect, analyze and use any and all data collected through the Telematics Services . . . ."[108] Therefore, while the LEAF owner technically owns the information, Nissan has essentially given itself a broad license to use the owner's data for various purposes. The issue here, once again, is whether there is informed consent. Suppose the customer accepted the "Terms of Use" upon registering the vehicle with CARWINGS. At this point, the agreement has now disappeared and the customer can no longer refer to it unless he or she has requested a copy from Nissan Customer Support.[109]

The FTC's Final Report provides the Commission's final

---

105. CARWINGS Agreement, *supra* note 8, ¶ 11.3. *See also* 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-16.

106. CARWINGS Agreement, *supra* note 8, ¶ 7.

107. *Id.* ¶ 11.1.

108. *Id.*

109. E-mail from Nissan EV Customer Support to author, *supra* note 34.

principle regarding consumers' access to data: "Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use."[110] LEAF owners who do have a copy of the CARWINGS Agreement will notice provisions regarding access to their data. The CARWINGS Agreement vaguely describes this as follows: "Nissan may at its option provide a website where [the LEAF owner] can access and review some of the data collected from [his or her] Nissan LEAF in connection with the Telematics Services."[111] And, "some" data is exactly what the owner gets. As discussed above, the owner has direct access to GPS location history from the vehicle's display screen. Yet, there are many more categories of data disclosed in the CARWINGS Agreement. The owner can obtain generalized data regarding driving behavior collected by CARWINGS by accessing the CARWINGS website through the Nissan Owner's Portal.[112] There is a lot of interesting information that can be viewed on the website, including annual and monthly distance traveled, average energy economy, electricity consumption and use, electricity captured by regenerative braking, and travel time.[113]

However, several of the more specific types of information mentioned earlier are nowhere to be found on the CARWINGS website. The concern here is whether or not the data that the LEAF owner does not have access to is sensitive enough to fall within the FTC's reasonable access requirement. This is difficult to determine when the consumer does not have a clear picture of all of the information that is being recorded and maintained. Clearly, if the CARWINGS website has the potential to collect geolocation data, such information has already been categorized as sensitive data by the FTC.[114] Further, federal regulations regarding vehicle identification number requirements describe VINs as unique identifiers.[115] Coupled with or linked to a specific person, this unique identifier could lead to or perhaps be in and of itself a form of personally identifiable

110. FTC REPORT, *supra* note 37, at 71.
111. CARWINGS Agreement, *supra* note 8, ¶ 8.
112. Password protected CARWINGS website, *supra* note 14.
113. *Id.*
114. FTC REPORT, *supra* note 37, at 15.
115. 49 C.F.R. § 565.15 (2008).

information.

The FTC, in its final framework, also recognizes the consumer's "right to be forgotten," specifically requesting not only that companies allow their customers access to their data under the proper circumstances, but that customers also be provided a way to suppress or delete the data where appropriate.[116] The CARWINGS Agreement does not contain provisions regarding the deletion of customer data. Neither is there a discernible way to remove the data that has already been made available to CARWINGS or information appearing on the user's CARWINGS website. The LEAF owner can discover how to delete information that appears on the vehicle's control screen either by looking through the different menu options or by reading the Owner's Manual. For example, stored destination and location items such as the driver's home address, vehicle address book, stored locations, stored routes, previous destinations, and areas to avoid can all be deleted from the vehicle's display screen settings menu.[117] Customers can also delete vehicle information from feed records, the numbers of incoming and outgoing telephone calls and data from a category broadly described as "vehicle information sharing" with Nissan through CARWINGS.[118]

Despite all of these numerous options for deleting certain types of data from the vehicle itself, a LEAF owner may not know how to determine what data is appropriate to delete. Unfortunately, customers would need to fully read and comprehend both the CARWINGS Agreement and Owner's Manual to understand why regular deletion of vehicle data would help to protect their privacy interests. From there, the consumer would need to balance his or her desire for convenience with privacy for items of information such as the stored address location. Some individuals, for example, may be unwilling to delete saved address book information or locational data because these features allow for greater convenience in future navigation. Others may decide to limit the information they enter into the system since, as stated above, deletion of data from the display screen does not alter information previously collected by CARWINGS.

---

116. FTC REPORT, *supra* note 37, at 23-24.

117. Photograph: 2011 Nissan LEAF Settings Control Screen, Vehicle Information (Francesca Svarcas, June 22, 2012) (on file with author).

118. Photograph: 2011 Nissan LEAF Settings Control Screen, Information Feed (Francesca Svarcas, June 22, 2012) (on file with author); Photograph: 2011 Nissan LEAF Settings Control Screen, CARWINGS (Francesca Svarcas, June 22, 2012) (on file with author).

G. Data Security

Nissan touts the use of "technical, physical and administrative safeguards" that protect the owner from theft, loss, misuse, improper distribution or alteration of data.[119] This includes the Nissan vehicle immobilizer system and vehicle security system (VSS).[120] The vehicle immobilizer system prevents the engine from starting unless a registered key is in close enough proximity to the vehicle.[121] Nissan achieves this by placing a chip inside the key.[122] While convenient, this solution presents serious security concerns. For example, the driver must never accidentally leave the key in the car because it is not possible to lock the keys in the car. It doesn't matter whether or not the key is left in plain sight. With the chip being close enough to activate the vehicle, a thief could enter the vehicle and take off with it. Not only would the thief get the car, but he or she would be able to access the owner's history of location data, telephone numbers dialed and answered through cell phone Bluetooth connections, and the address book, unless the vehicle owner recently deleted each category of data just before leaving the car.

The VSS "provides visual and audio alarm signals if someone opens the doors, or rear hatch when the system is armed."[123] Nissan admits that this system "helps deter vehicle theft but cannot prevent it, nor can it prevent the theft of interior or exterior vehicle components in all situations."[124] As illustrated in terms of the vehicle immobilizer system, this is particularly true for privacy and security regarding the interior vehicle components.

Theft of certain data occurring outside of the vehicle at least has the protection of being encrypted. Nissan encrypts what it calls "sensitive information," such as location information, credit card

---

119. CARWINGS Agreement, *supra* note 8, ¶ 11.4.

120. 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 2-35.

121. *See id.* at 2-36, 3-2. The recently enacted Moving Ahead for Progress in the 21st Century Act (MAP-21) initially included Section 31405 regarding standards for pushbutton ignition systems. S. 1813, 112th Cong. § 31405 (2012), *available at* http://www.govtrack.us/congress/bills/112/s1813/text. However, a later version of MAP-21 regarding vehicle electronics and safety standards dropped this section. H.R. 4348, 112th Cong. (2012), *available at* http://www.rules.house.gov/Media/file/PDF_112_2/LegislativeText/CRPT-112hrpt-HR4348.pdf.

122. *Id.* at 3-2.

123. 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 2-35.

124. *Id.*

information, usernames, and passwords.[125] This seemingly comports with the FTC's required protections for financial information and geolocation data at least as far as GPS transmissions from the vehicle to CARWINGS are concerned.[126] For some period of time, however, an inconsistency remained with respect to a representation regarding encryption of location information in a system where locational data could be transmitted to RSS providers in plaintext via the RSS URL.[127] Thinking back to the LEAF owner who experimented with his RSS feed settings in CARWINGS,[128] if an RSS provider could see where its subscriber was driving, what good would it have been for locational data to be otherwise encrypted? Moreover, one wonders whether any unencrypted data sent over RSS feeds was later stored by RSS providers. Nissan's response to the article disclosing the RSS leak was not that this was or should also be encrypted, but that the data sharing was ultimately in the hands of the user who had a choice of whether or not to opt in.[129] As discussed above, the CARWINGS Agreement does not disclose CARWINGS' or Nissan's use of RSS technology at all, let alone the ability of the LEAF to transmit data to an RSS provider. Nissan's more general online privacy policy also makes no mention of RSS data or devices.[130] Accordingly, neither document contains a disclosure as to whether or not RSS communications that the vehicle transmits to the RSS provider are just as non-encrypted as the RSS broadcast.

Perhaps this is because Nissan has conscientiously, albeit surreptitiously, fixed the problem.[131] On July 10, 2012 computer science graduate David Gobaud[132] created a Ruby on Rails[133] website

125. CARWINGS Agreement, *supra* note 8, ¶ 11.4.

126. FTC REPORT, *supra* note 37, at 15-16.

127. *See* CARWINGS Agreement, *supra* note 8, ¶ 11.4 (encryption of location information); Niedermeyer, *supra* note 21 (discussing unencrypted location information leaked via RSS).

128. *See supra* note 21 and accompanying text.

129. Niedermeyer, *supra* note 21.

130. *See Privacy Policy*, *supra* note 39.

131. *See Nissan LEAF CARWINGS RSS Privacy Issue*, YOUTUBE (June 12, 2011), http://www.youtube.com/watch?feature=player_embedded&v=taZ7fjgPRCI (containing a link to http://nwrs.net/carwings.php, which displays the following message: "Now that nissan [sic] has fixed the problem, this RSS feed no longer is needed.").

132. The author gives special thanks to David Gobaud, B.S., Stanford University, who set up the website and inspected the log requests, and to Michael Stolte, J.D. Candidate at the University of California, Hastings College of the Law, who assisted with observation and photo documentation.

with an RSS feed to verify that the LEAF's CARWINGS RSS client no longer transmits the vehicle's GPS location to the RSS server via the query string portion of the Hypertext Transfer Protocol (HTTP) request. He then hosted the website on Heroku[134] and used Papertrail[135] to monitor the logs. The author and owner of the tested vehicle, a 2011 Nissan LEAF purchased in June of 2011, then entered the RSS feed URL as a new Internet feed on the CARWINGS website, giving the feed the name "Test Drive."[136] After refreshing the news feed from within the vehicle, Test Drive appeared as a feed on the vehicle's control panel under "Favorites."[137] On July 11 and 12, 2012, the author connected to the RSS feed through the vehicle multiple times. The requests observed in the server logs contained information about the dates, times and numbers of requests made, but did not contain GPS location data.

H. Other Entities' Collection of Data Glossed Over by Broad Releases of Liability

The CARWINGS Agreement does not have specific terms or provisions regarding other entities' collection of LEAF owners' data. The provisions regarding disclosure of data to others, paired with how the information is being used, are not enough to fully inform the consumer about third party data use. It would make sense for emergency responders and service providers such as the police, fire department and ambulance personnel to be using the user's location information collected via GPS to get to the scene of an accident. Yet, once the data has been shared with "any person, company, subsidiaries or affiliates . . . [acting] in connection" with the telematics services,[138] serious questions are raised with respect to the collection and further use of that data.

Given the transfer of all of the various types of information over

---

133. RUBY ON RAILS, http://rubyonrails.org (last visited July 12, 2012) (web framework).

134. HEROKU, http://www.heroku.com (last visited July 12, 2012) (cloud application platform).

135. PAPERTRAIL, https://papertrailapp.com (last visited July 12, 2012) (hosted log management application).

136. Password protected CARWINGS website, *supra* note 14.

137. Photograph: 2011 Nissan LEAF CARWINGS Control Screen, Favorite Feed (Francesca Svarcas, June 22, 2012) (on file with author).

138. *See* CARWINGS Agreement, *supra* note 8, ¶ 7. *See also* 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-16.

wireless and satellite networks, the CARWINGS Agreement contains a provision that the owner agrees to release Nissan of liability for any damages resulting from said channels of communication.[139] In fact, Nissan sets its maximum liability to the owner under any theory or claim, including consumer protection and right of privacy, at $250.[140] The LEAF owner also contracts that he or she releases the wireless carriers of liability, including claims in contract, warranty, negligence, strict liability and tort.[141] And, even though the customer owns the vehicle and all rights in the data collected by the vehicle, the agreement states that the owner has no right in the wireless phone number assigned to the LEAF.[142] It is unclear whether Nissan owns that number or if ownership remains with Nissan's wireless carrier, AT&T,[143] or some other entity. Therefore, from Nissan's standpoint, it apparently is of no consequence who, aside from Nissan, collects the LEAF owner's data, whether through Nissan's sharing of the data or some other means of retrieval of the unencrypted data. RSS providers, for example, may very well fall within the broad category of "any person, company, subsidiaries or affiliates . . . in connection" with the vehicle's telematics.[144]

Despite all of the broad releases afforded to both Nissan and its wireless carriers in the CARWINGS Agreement, Nissan does not offer its customers any warranties for the telematics services.[145] Perhaps this is because Nissan could argue that the preliminary three-year contract is not for an additional paid service.[146] As if the provisions for broad releases and lack of warranty were not enough, the Agreement provides Nissan the protection of being able to terminate or suspend the telematics services.[147] There are likewise

139. CARWINGS Agreement, *supra* note 8, ¶ 11.2.

140. *Id.* ¶ 15.3.

141. *Id.* ¶ 13.

142. *Id.*

143. *See* sources cited *supra* note 94.

144. CARWINGS Agreement, *supra* note 8, ¶ 7. Even though RSS providers no longer appear to receive geolocation data from subscribers connecting through the vehicle, the RSS provider likely keeps track of some data such as the date, time and frequency of requests and connections made.

145. *Id.* ¶ 14.

146. *Id.* ¶¶ 1, 3. Note that the three-year subscription has been characterized as being part of the vehicle's purchase price, which technically may not be free.

147. *Id.* ¶ 17 (termination can occur without cause upon thirty-day notice or for good cause without notice).

provisions, in the customer's favor, for deactivating and canceling the telematics services either permanently through the Owner's Portal or by calling Nissan, or temporarily by either changing certain settings within the navigation system itself or selecting "Decline" on the pop-up consent screen.[148] However, an owner should reasonably expect that terminating the agreement would be a last resort effort rather than the only recourse. The benefits and conveniences of the telematics system were conceivably strong factors in leading the consumer to purchase the vehicle in the first place.[149] One critical benefit of CARWINGS is that it directs the driver to nearby charging stations.[150] This is tremendously useful on longer trips given that the vehicle has only an estimated 100-mile range when fully charged.

The Owner's Manual states that in not accepting the terms of the pop-up consent screen "certain features of [the] vehicle which are dependent on the vehicle telematics will not operate as intended or designed."[151] It is not clear what this means, but given the lack of information provided, this could potentially include the benefit of finding charging stations within the vehicle's mileage range. The CARWINGS Agreement provides no further clarification, stating only that the owner "can turn off the transmission of certain categories of data by pressing the 'Decline' button in the pop-up message . . . ."[152] and warning that "If you click on the 'Decline' button, your use of the telematics services will be very limited."[153] Turning off the "Vehicle Information Sharing with Nissan" option in the navigation system only disables "automatic sharing of information at vehicle ignition. Certain categories of data may still be transmitted if certain Telematics Services features are accessed either in the vehicle or remotely."[154] The Navigation System Owner's Manual, a volume separate from the Owner's Manual, provides that

148. *Id.* ¶ 4.

149. *See* FTC REPORT, *supra* note 37, at 50-51. The commenters of the FTC's proposed framework issued in December 2010 analyzed whether or not a product or service is essential in determining the appropriateness of take-it-or-leave-it choice for the collection of consumer data. *Id.* The FTC agreed that a take-it-or-leave-it approach to consent presents privacy concerns to the extent that the information is being collected "in a manner inconsistent with the context of the interaction between the business and the consumer." *Id.* at 51.

150. 2011 LEAF NAVIGATION SYSTEM OWNER'S MANUAL, *supra* note 11, *passim*.

151. 2011 LEAF OWNER'S MANUAL REVISED, *supra* note 6, at 9-16.

152. CARWINGS Agreement, *supra* note 8, ¶ 4.

153. *Id.* at para. 4 (original in all caps).

154. *Id.* ¶ 4.

"[n]avigation functions, audio, hands-free phone, vehicle information display, etc. can still be operated even if [Decline] is touched."[155] The manual subsequently limits navigation functions to the "static navigation system."[156]

V. CONSTITUTIONAL CONSIDERATIONS REGARDING CARWINGS COLLECTION AND USE OF EV DATA

As shown above, from the consumer's standpoint there are significant problems with several provisions in the CARWINGS Agreement as well as validity concerns surrounding the pop-up consent screen. Even if the questionable portions of the agreement and the pop-up screen were to be upheld as contractually valid and enforceable, there are certain constitutional protections for individuals' privacy rights that would apply to the collection and transmission of personal data. There is a common law history of the United States Supreme Court opinions that analyze electronic and enhanced surveillance technologies in terms of the Fourth Amendment. Among these are *United States v. Knotts*,[157] which involved the tracking of routes traveled by an automobile via a beeper placed in a drum of chloroform,[158] and the more recent opinion of *United States v. Jones*[159] where police officers placed a GPS device on a vehicle to track the driver's whereabouts.[160]

A. Existing Constitutional and Industrial Climates

Knotts analyzed the beeper technology both under the reasonable expectations standard derived from *Katz v. United States*,[161] and traced precedent that did not require a physical trespass or intrusion.[162] The Court came to the conclusion that "monitoring the beeper signals . . . [did not] invade any legitimate expectation of privacy"[163] because "the type of information revealed by the beeper

155. 2011 LEAF NAVIGATION SYSTEM OWNER'S MANUAL, *supra* note 11, at 1-5 (second set of brackets in original).

156. *Id.* at 5-3.

157. 460 U.S. 276 (1983).

158. *Id.* at 278.

159. 132 S. Ct. 945 (2012).

160. *Id.* at 948.

161. 389 U.S. 347 (1967).

162. *Knotts*, 460 U.S. at 280-85.

163. *Id.* at 285.

did not exceed that which could have been discovered through unaided observation."[164] The focus in *Jones*, however, was the occurrence of a physical intrusion—the actual placement of the transmitting device in or on the vehicle—that constituted the privacy violation.[165] The *Jones* opinion acknowledged, but left open the question of whether "achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy . . . ."[166] Therefore, protections regarding the wireless transmission of GPS data from preinstalled devices are not yet decided or defined in the context of vehicles.

There is some case law regarding the use of data collected from EDRs being used in criminal trials, but the analysis has mainly focused on admissibility requirements, the scientific probative value of the data, and its interpretation by expert witnesses.[167] Specific to privacy, a California court of appeal found a criminal defendant to have a reasonable expectation of privacy in his EDR data under the Fourth Amendment, but the case has since been depublished and is no longer citable.[168] Further, the government and insurance companies are proponents of the use of EDR data.[169] National Highway Traffic Safety Administration (NHTSA), for example, has imposed standards regarding mandatory EDR data elements and reporting format, as well as for the collection and recording of such information.[170] And, insurance companies have already submitted EDR data as evidence in civil trials.[171] Fortunately, most car manufacturers encrypt EDR data, so even if transmitted wirelessly, the recipient would need to be sophisticated enough to be able to do anything with it.[172]

The novel issue of data transmissions from vehicles to RSS providers has not come up in courts at all.[173] Given the rising use of

---

164. Hutchins, *supra* note 10, at 435.

165. *Jones*, 132 S. Ct. 948.

166. *Id.* at 954.

167. *See* Askland, *supra* note 7, at 3-4. *See also* Glancy, *supra* note 9.

168. People v. Xinos, 121 Cal. Rptr. 3d 496 (Ct. App. 2011) (depublished). *See also* Peter R. Thom, *The Black Box*, CALIFORNIA LAWYER (March 2012), *available at* http://www.callawyer.com/Clstory.cfm?eid=920908.

169. *See* Askland, *supra* note 7, at 4-6; Glancy, *supra* note 9.

170. 49 C.F.R. §§ 563.7 to .9 (2011).

171. Askland, *supra* note 7, at 5-6.

172. *Id.* at 6.

173. Cases that mention RSS feeds tend to do so in the context of intellectual property infringement. *See, e.g.*, Ceiva Logic, Inc. v. Frame Media, Inc., No. SACV 08-00636-JVS

electric vehicles and the prevalence of more and more wireless technology being included in automobiles as much sought after features, privacy invasions regarding the wireless transmission of data may very well appear in front of the United States Supreme Court in the future. When the Court is required to address the constitutionality of data collected and transmitted electronically, it will be interesting to see what avenue it takes in terms of drawing upon past precedent and authority.

B. Future Privacy Considerations Regarding Current Technology

One question the Court may consider is whether or not information collected from preinstalled devices or onboard units qualify as physical intrusions without the added physical trespass of a governmental entity.[174] If, for example, NHTSA or some other governmental agency were to require GPS and RSS devices to be standardized and installed in all vehicles, similar to how EDRs have become regulated, would this be enough of a government intrusion? Unless the Court returns to the *Katz* analysis of reasonable expectations of privacy regarding people, rather than places, the answer is likely no.[175] Moreover, in terms of GPS equipment, the Federal Communications Commission's intention as early as February 2004 was to expand the use of GPS onboard vehicles and facilitate communications between these units and roadside units.[176]

Another approach the Court may take is via some form of derivative application of *Kyllo v. United States*.[177] *Kyllo* involved the use of thermal imaging devices to detect marijuana in a person's home, which the Court struck down as unconstitutional.[178] The most likely hurdle here is that the Court has already decided that persons' homes are afforded greater privacy protections than public places,[179] including the confines of one's automobile. However, if this case were to be more broadly construed in terms of enhanced surveillance

(RNBx), 2009 WL 7844245 (C.D. Cal. June 9, 2009); Righthaven LLC v. Choudhry, No. 2:10-CV-2155 JCM (PAL), 2011 WL 2976800 (D. Nev. July 21, 2011).

174. *See generally* United States v. Jones, 132 S. Ct. 945 (2012).

175. *See* Katz v. United States, 389 U.S. 347 (1967).

176. Glancy, *supra* note 3, at 311.

177. 533 U.S. 27 (2001).

178. *Id.* at 29, 40.

179. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

methods in general, the ultimate result would be similar to *Katz*'s reasonable expectation analysis of "people, not places,"[180] albeit in a more roundabout way. It is, after all, Justice Scalia who said, "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[181] It logically follows that the more advanced the technology becomes, the greater the impact will be on individuals' privacy, regardless of where they may be.

It is only a matter of time before the lines between a person's home and his or her ventures out into society become meaningfully blurred by advances in technology. Take, for instance, the means by which a LEAF owner can charge the vehicle's batteries. One way is to go to a charging station where the driver can pay to connect the vehicle to an electrical outlet. This is useful on days where the owner's driving distance exceeds the vehicle's estimated driving range. Typically, however, the driver will want to keep track of the battery charge and connect the vehicle to a charging station at his or her own home. Recall that one of the benefits of purchasing an electric vehicle is to avoid gas stations, whether it is due to the high gas prices, desire for convenience, or both. Some amount of the discussion about the wireless technology in the LEAF also applies to home-based charging stations. The charging station mounts to a wall inside the owner's garage, technically within the person's home. The charging station then wirelessly transmits information to the owner of the equipment such as when and for how long the vehicle is being charged. At this point, the "electronic," or nonphysical,[182] intrusion, absent of any physical trespass, falls within the private sanctity of the home.[183]

The federal courts may also consider drawing persuasive authority from state privacy laws. California, for example, has both privacy torts and a cause of action for constructive invasion of privacy. Privacy torts, such as intrusion based on electronic

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

181. *Kyllo*, 533 U.S. at 33-34.

182. This is in contrast to the physical intrusion discussed in *Jones*, and in comparison with the thermal imaging of *Kyllo*. Although there is a possibility that wireless transmission could be considered scientifically "physical," this discussion is outside the scope of this article.

183. Since the charging station is from a company other than Nissan and is not a known party to or beneficiary of the CARWINGS Agreement, the purpose of mentioning the charging station is intended as illustrative rather than a topic for further analysis in this article.

surveillance, require the intrusion to be "highly offensive."[184] This is a high, not to mention fact-dependent, bar to prove in most cases.[185] Perhaps more alarming is the idea that what citizens consider highly offensive today may fluctuate due to complacency and surrender to more sophisticated technologies, thereby raising the bar even higher.[186] There is already a certain comfort associated with the convenience of electronic Wi-Fi gadgets, and through increased use individuals may, as Justice Alito noted in *Jones*, "at the expense of privacy . . . find the tradeoff worthwhile."[187] Ongoing observations regarding online social networking practices of teenagers and young adults reveal the habitual sharing of private information by a younger generation with a much greater confidence in, or perhaps obliviousness to, data collecting and transmitting technology than that of their parents.[188]

An analysis similar to or derived from California's constructive invasion of privacy cause of action may be more promising.[189] To state a cause of action under constructive invasion of privacy a showing of physical trespass—as was required by the Supreme Court in *Jones*—is not necessary, and the harmful conduct must be offensive to a reasonable person, rather than highly offensive.[190] California's statute provides:

> A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or

184. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

185. *See* Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 21 (2007) (describing "highly offensive" as a difficult determination that depends on multiple factors including "historical moment, class, culture, education, and other moving sociological targets").

186. *Id.*

187. United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring in judgment).

188. *See* AMANDA LENHART & MARY MADDEN, PEW INTERNET & AM. LIFE PROJECT, TEENS, PRIVACY & ONLINE SOCIAL NETWORKS, at i-vii (2007), *available at* http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.pdf. *See also* Stephanie Graziano, *Social Media Privacy Implications for Teens*, INFOSEC ISLAND (Mar. 27, 2011), http://infosecisland.com/blogview/12693-Social-Media-Privacy-Implications-for-Teens.html.

189. *See* CAL. CIV. CODE § 1708.8(b) (West 2010). *See also* Glancy, *supra* note 3, at 374.

190. CAL. CIV. CODE § 1708.8(b) (West 2010).

> familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.[191]

The cited code section, applied to the electronic transmissions discussed in this article, seems to require something more than textual transmissions of data. The statute references the capture of data through visual or auditory enhancing devices. However, as seen above, non-pictorial data can paint as detailed a picture. Suppose, for instance, a family is together on an extensive road trip in their shiny new electric vehicle. The children take turns playing their favorite MP3s using the USB ports provided in the vehicle. Mom and dad, insisting on a break from the booming bass beats, tune into their news stations through RSS feeds they have added to CARWINGS. Meanwhile, the telematics system has been tracking the vehicle's speed, stops taken at multiple EV charging stations, and an incoming telephone call from grandma, not to mention EDR data of dad's near miss of a collision with a semi-trailer truck while passing through Somerset, Pennsylvania at the precise location of +40° 0' 39.08", -79° 6' 50.64". The electronic transmission of data collected by the telematics system and shared with unknown third parties under these circumstances is arguably just as effective as a wiretap or hidden video camera capturing the same scene.

Also, keeping in mind that third parties such as wireless carriers and the media are nongovernmental entities, the standards for which the information can be used are going to be different than if the police or other government body were capturing the data. Again, using California constitutional privacy law as example, noncriminal privacy litigation differs in that nongovernment entities do not need to show a "compelling interest" with respect to the purposes for which the information is being collected and used.[192] They only need to show that the interest is "legitimate" or "important."[193] The question here

---

191. *Id.*

192. Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 668 (Cal. 1994) (en banc).

193. *Id.* at 656, 668 (describing "legitimate" interests as those "derive[d] from the legally authorized and socially beneficial activities of government and private entities" and determining the "importance" of such interests "by their proximity to the central functions of a particular public or private enterprise").

becomes whether or not Nissan's disclosures are made to others who have a legitimate interest with respect to the purposes for which the data is being used. Roadside assistance and emergency service providers have an important enough interest in assisting at the scene of an accident. However, entities from the media industry, such as news stations that offer RSS feeds, have no conceivable interest in retaining data that at one time revealed the driver's speed or location.

VI. CONCLUSION

American author Stewart Brand has been known to say that "[o]nce a new technology rolls over you, if you're not part of the steamroller, you're part of the road."[194] Since the 2001 *Kyllo* decision, newer and more powerful technologies for electronic devices exist and are being used in ways that, if left unaddressed, could greatly impact individuals' privacy rights. The telematics system of the Nissan LEAF is just one example, with a new era of self-driving autonomous vehicles at our doorsteps.[195] The steamrollers from which citizens need protection are clearly becoming exponentially larger and more aggressive. Nevertheless, the majority in *United States v. Jones* left unresolved the question of whether wireless transmissions of data collected by onboard devices would constitute an unconstitutional invasion of privacy. If individuals reconcile themselves to lesser degrees of privacy associated with these new technologies, then they, in tandem with the institutions charged with protecting their privacy, face the upcoming hazards of becoming "part of the road."

194. *Steamroller Quotes: Stewart Brand*, BRAINY QUOTE, http://www.brainyquote.com/quotes/keywords/steamroller.html (last visited Oct. 12, 2012).

195. *See* James Temple, *California Senator Rolls Out Autonomous Vehicle Bill, Rolls Up in Google Car*, SFGATE (Mar. 1, 2012, 7:55 AM), http://blog.sfgate.com/techchron/2012/03/01/california-senator-rolls-out-autonomous-vehicle-bill-rolls-up-in-google-car/.