UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 18 | Issue 5 Article 7

4-1-2017

The Security and Privacy In Your Car Act: Will It Actually Protect You?

Benjamin L. Bollinger

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 18, ISSUE ON.: APRIL 2017

THE SECURITY AND PRIVACY IN YOUR CAR ACT: WILL IT ACTUALLY PROTECT YOU?

Benjamin L. Bollinger*

On July 21, 2015, in light of emerging technology involving autonomous driving vehicles, the United States Senate proposed Senate Bill 1806, or the Security and Privacy in Your Car Act, to address issues surrounding these technologies. The "SPY Car Act" attempts to address issues surrounding cybersecurity, data privacy, and hacking of autonomous driving vehicles. The Senate Committee on Commerce, Science, and Transportation is currently analyzing the SPY Car Act. If enacted, this bill could pave the way for the autonomous driving vehicle industry to be effectively regulated. Although this bill has its shortcomings, it is a good start to the conversation regarding the privacy and security concerns associated with autonomous driving vehicles.

I. INTRODUCTION

For most drivers who have sat steaming in rush hour traffic or wished they could catch up on work instead of driving in to the office, self-driving cars may be an enticing option. With the emergence of these vehicles, the concerns over vehicle safety, data security, data privacy, and regulation are at the forefront of the minds of industry and government actors. This Recent Development analyzes the Security and Privacy in Your Car Act ("SPY Car Act"), a bill before Congress that seeks to govern cybersecurity and privacy aspects of self-driving vehicles, and examines how this legislation will address the concerns surrounding this emerging technology.

Autonomous driving vehicles, also known as self-driving vehicles, are on the verge of becoming an everyday sight on roads.[1] While these vehicles would definitely provide drivers with many advantages,[2] they also come with considerable risks and liabilities.[3]

---

* J.D. Candidate, University of North Carolina School of Law, 2018. I would like to thank Professor Anne Klinefelter and the North Carolina Journal of Law and Technology for all of their help with this article.

[1] BI Intelligence, *Ten Million Self-Driving Cars Will Be on the Road by 2020*, BUSINESS INSIDER (June 15, 2016), http://www.businessinsider.com/report-10-million-self-driving-cars-will-be-on-the-road-by-2020-2015-5-6 (stating that by the year 2020 there will be close to 10 million vehicles on the road that will have some sort of self-driving technology incorporated within the vehicle).

[2] *See* Dan McLaughlin, *17 Ways Driverless Cars Could Change America*, THE FEDERALIST (July 16, 2014), http://thefederalist.com/2014/07/16/17-ways-driverless-cars-could-change-america/ (listing fewer car accidents, changing of traffic patterns, changing the insurance and legal culture, and changing the layout of cities as the many effects of self-driving vehicles).

Cybersecurity and privacy risks have the potential to delay, or even break, the self-driving vehicle industry.[4] Although it may be the industry's intention to put the safest and most reliable vehicles on the road, the federal government must implement regulations to protect consumers and govern this emerging and complex technology.

Cybersecurity and data privacy are some of the most significant areas of concern arising from self-driving vehicles. These apprehensions stem from the knowledge that self-driving vehicles will rely on some combination of Internet-based communication systems to operate the vehicles without the control of a human driver.[5] Furthermore, because these vehicles will invariably be connected to the Internet, there are risks that the wireless connection could be breached and the vehicles' operating system could be interfered with or sensitive personal data being transmitted over the connection could be stolen.[6]

While it may seem that cybersecurity and data privacy are intermingled issues, they must be viewed as separate and distinct.[7] The SPY Car Act's definition of cybersecurity includes differing elements that must be distinguished from the definition of data

---

[3] *See* Tia Ghose, *Self-Driving Cars: 5 Problems That Need Solutions*, LIVE SCIENCE (May 14, 2015), http://www.livescience.com/50841-future-of-driverless-cars.html.

[4] RAND Corporation, AUTONOMOUS VEHICLE TECHNOLOGY: A GUIDE FOR POLICYMAKERS 94 (2016) (stating that the privacy concerns surrounding autonomous vehicles "could potentially derail the business").

[5] *Id.* at XIX–XXII (explaining how these vehicles could potentially rely on "cloud-based resources," "vehicle to vehicle" communication ("V2V"), "vehicle to infrastructure" communication ("V2I"), GPS technology, and "inertial navigation systems ("INS"). This report also states that software upgrades for the vehicle over the Internet may also pose problems for the industry.

[6] *Id.* at 6. (stating "Internet-connected systems might be hacked by the malicious.").

[7] It is important to delineate the two terms because of the tendency to confuse them. A breach of cybersecurity can be viewed as a breach of privacy, and a breach of privacy can be viewed as a breach of cybersecurity. However, the SPY Car Act uses specific language to show what is included under each definition, and this Recent Development will adhere to those definitions.

privacy.[8] Cybersecurity is defined by the SPY Car Act as protection against hacking of all "entry points to the electronic systems of each motor vehicle."[9] "Entry points" into the vehicle are any wireless or wired connection through which "control signals" travel or a connection through which data can be "accessed directly or indirectly."[10] The SPY Car Act also relates cybersecurity to the protection of "software systems that can affect the driver's control of the vehicle movement."[11]

Conversely, the SPY Car Act defines data privacy much more narrowly. Here, data privacy is limited to notice, transparency, consumer control, and limitation on the use of data collected by manufacturers.[12] These definitions clearly delineate between the two terms. The definition of cybersecurity used in the SPY Car Act refers to two things: (1) the protection against malicious interference with the self-driving vehicle's operability;[13] and (2) unauthorized access to or interception of driving data.[14] On the other hand, the definition of data privacy refers to what manufacturers can and cannot do with harvested driving data and the right of the consumers to that data.[15]

---

[8] Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. (2015). The SPY Car Act's definition of cybersecurity can be split into two separate elements: protection against an attempt to take control of the vehicle's driving ability and protection against stealing or intercepting of driving data. The data privacy definition speaks to the scenario where the manufacturer is mining data and what they can do with it and what rights the consumer has to the mining and use of the data.

[9] *Id.* at 3.

[10] *Id.*

[11] *Id.* at 2.

[12] *Id.* at 8–11.

[13] This is evidenced by the inclusion of the "protection against hacking" language and while someone may hack driving data the Senate also includes that hacking can be unauthorized access to the "electronic controls" of the vehicle. *See id.* at 3.

[14] This is evidenced by the inclusion of "unauthorized access to . . . driving data" in the definition of "hacking" and the "protection against hacking" provision and the "security of collected information" section of the cybersecurity standards portion. *See* Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. 3 (2015).

[15] *Id.* at 8–11.

The difference between cybersecurity and data privacy is further illustrated by the differing risks of harm from breaches. An example of a cybersecurity breach is where a vehicle's operating system is hacked.[16] In such instances, a hacker may be able to "take over the brakes, engine, or other components of a person's car."[17] This is concerning because such breaches of security could result in serious bodily injury or death. However, in the event of a privacy breach, where a driver's personal data are vulnerable, the consequences could have other impacts on the consumer.[18] The data retained by vehicle manufacturers are so sensitive, if a consumer's data privacy is breached and the information is transferred to an unauthorized third party, the third party could potentially track a consumer's whereabouts, anticipate a consumer's movements, or potentially implicate a consumer by leaking proof of illegal conduct based on a consumer's movement.[19] This could lead to reputational harms, loss of employment, and loss of liberty.[20]

Cybersecurity and privacy standards for self-driving vehicles are still evolving.[21] The U.S. Department of Transportation has recognized the fact that no standards exist for self-driving vehicle

---

[16] *See* Kevin Collier, *How Easy is it to Hack A Self-Driving Car?,* VOCATIV (June 29, 2016), http://www.vocativ.com/332734/driverless-car-hack/.

[17] Tom Simonite, *Your Future Self-Driving Car Will Be Way More Hackable*, MIT TECH. REV. (Jan. 26, 2016), https://www.technologyreview.com/s/546086/your-future-self-driving-car-will-be-way-more-hackable/. *See also* Alex Hern, *Car Hacking Is the Future—and Sooner Or Later You'll Be Hit*, THE GUARDIAN (Aug. 28, 2016), https://www.theguardian.com/technology/2016/aug/28/car-hacking-future-self-driving-security.

[18] *See infra* note 48.

[19] *See generally* Mathew Gillespie, *Shifting Automotive Landscapes: Privacy and the Right to Travel in the Era of the Autonomous Motor Vehicles*, 50 WASH. U. J.L. & POL'Y 147 (2016) (discussing the potential privacy risks inherent in autonomous driving vehicles).

[20] *See* Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 151 (1995) (discussing how intelligent transportation technology can potentially affect the privacy rights of consumers).

[21] U.S. Department of Transportation, FEDERAL AUTOMATED VEHICLES POLICY 21 (2016).

manufacturers to use to model their industry practices and that "more research is necessary before proposing a regulatory standard." [22] The industry cannot mass-produce self-driving vehicles until industry standards and federal regulations exist.[23] These standards and regulations are important to mass-production because of the potential for widespread harm.

In response to these concerns, the U.S. Congress proposed the SPY Car Act in July 2015.[24] This Recent Development analyzes the provisions of the SPY Car Act with existing data privacy regulations and argues that the United States Senate has not completely addressed every issue pertaining to self-driving vehicles. Part II discusses the relevant law in the arena of privacy regulation. Part III elaborates on the SPY Car Act and the issues it addresses, such as "hacking," "cybersecurity standards," "cyber dashboard," and "privacy standards,"[25] with a particular focus on the privacy provisions. Part IV analyzes the privacy provisions of the SPY Car Act and whether a particular provision will help to reconcile privacy concerns. Finally, Part V suggests recommendations for how the SPY Car Act can be improved to better address the issue of privacy surrounding self-driving vehicles.

II. RELEVANT PRIVACY LAW

Before discussing relevant privacy law, it is important to note the federal entities that will play a pivotal role in governing vehicles of this nature. Because the regulation of these vehicles will involve two separate forms of governance, the actual vehicle itself and the Internet-based operational features, the SPY Car Act requires the National Highway Traffic Safety Administration ("NHTSA") and the Federal Trade Commission ("FTC") to consult with each other before issuing any regulations.[26] First, the U.S. Department of Transportation ("DOT"), through the NHTSA,

[22] *Id.*
[23] RAND, *supra* note 4.
[24] Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. (2015).
[25] *Id.* at 3–11.
[26] *Id.* at 5–7, 10–11.

governs all road vehicles within the United States.[27] The NHTSA has the power to promulgate Federal Motor Vehicle Safety Standards ("FMVSS") with which vehicle manufacturers must certify compliance.[28] Furthermore, even with the lack of FMVSS standards for self-driving vehicles,[29] the NHTSA still has the "authority to identify safety defects, allowing the [NHTSA] to recall vehicles or equipment that pose an unreasonable risk to safety."[30] This is important because it creates a potential safeguard against defective and dangerous vehicles being operated while the federal government is still trying to issue regulations for these new vehicles.

In addition, with the high degree of wireless technologies[31] in self-driving vehicles, the FTC will be a major player that will need to work in conjunction with the NHTSA to achieve strong regulations for self-driving vehicles.[32] The FTC will operate in a consulting capacity for cybersecurity standards [33] and cyber dashboard [34] rulemaking and will hold primary rulemaking authority on the privacy standards[35] for self-driving vehicles.

---

[27] 49 U.S.C. § 105 (2016).

[28] 49 U.S.C. § 30101 (2016).

[29] The current statutory definition for a motor vehicle does not include any provision for self-driving vehicles. The current definition for "'motor vehicle' means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways [.]" *See id.* § 30102.

[30] U.S. Department of Transportation, *supra* note 21, at 7.

[31] *See* Dorothy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J. 1617, 1627–40 (2014) (discussing connected vehicle technologies and how the USDOT "recognizes two main categories or types of vehicular communications: (1) Connected Vehicles Safety Systems that use Dedicated Short Range Communications ("DSRC") transceivers to send and receive vehicle status communications; and (2) Connected Vehicle Mobility Applications that generally use cellular wireless to send and receive a wide range of data, from the status of the vehicle, to navigation assistance and infotainment").

[32] The U.S. Senate recognizes the importance of the FTC as a cohort in formulating regulations, which is evidenced by the inclusion of the FTC in the SPY Car Act. *See* Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. 2, 5–8, 10–11 (2015).

[33] *Id.* at 5.

[34] *Id.* at 7. The "cyber dashboard" is essentially an affixed notice on a manufactured vehicle which contains information for the consumer regarding

As discussed previously, self-driving vehicles will rely on some form of communication and operating technology that will utilize the Internet.[36] Because no current regulation establishes privacy standards for these vehicles, this Recent Development will analyze the SPY Car Act using the lens of the Fair Information Practices ("FIPs"). The FIPs were created by the Department of Health, Education and Welfare "in response to growing use of automated data systems containing information about individuals."[37] The FIPs are highly influential guidelines in privacy laws that have been cited by the FTC in relation to its regulatory authority under the Federal Trade Commission Act ("FTCA").

A. The Fair Information Practices

The FTC, considered a major actor in U.S. privacy regulation, issued a report to Congress in 1998 that laid out what the FTC called the "five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress."[38] Although, historically, the United States' privacy laws have not consistently reflected these core principles,[39] the "FIPs are important because they provide the underlying policy for many national laws addressing privacy and data protection matters."[40] This section analyzes the privacy portion of the SPY Car Act against the FIPs to determine if the SPY Car Act will be successful in accomplishing

---

the measures the vehicle takes to protect the cybersecurity and privacy of the vehicle and the consumer.

[35] *Id.* at 10.

[36] *See* RAND, *supra* note 4.

[37] Robert Gellman, *Fair Information Practices: A Basic History*, 2 (Version 2.17 2016). *See also Records, Computers, and the Rights of Citizens*, a report of the Secretary's Advisory Committee on Automated Personal Data Systems U.S. Department of Health, Education, and Welfare, July 1973 DHEW Publication No. (OS) 73-94.

[38] Federal Trade Commission, *Privacy Online: A Report to Congress* 7 (1998).

[39] *See* Gellman, *supra* note 37, at 1 ("Privacy laws in the United States, which are much less comprehensive in scope than laws in some other countries, often reflect some elements of FIPs but not as consistently as the laws of most other nations.").

[40] *Id.*

its stated purpose. The following subsections will go into greater detail on the five FIPs and will illustrate how each individual principle is relevant to self-driving vehicle technology.

1. Notice/Awareness

The first and "most fundamental principle" is notice.[41] The FTC states "consumers should be given notice of an entity's information practices before any personal information is collected from them."[42] This principle is relevant to self-driving cars because of the high value of the information gathered by the vehicle and the possibility that data obtained from the vehicle could potentially contain personal data regarding the passengers.[43] The FTC states that "[w]ithout notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information." [44] A consumer's decision to disclose personal information might be made for them, without notice, as the nature of the data collected by the vehicle will reveal some personal information about the vehicle's passengers.[45]

2. Choice/Consent

The second FIP is consumer choice or consent.[46] The FTC defines "choice" as "giving consumers options as to how any personal information collected from them may be used."[47] The Federal Automated Vehicles Policy states that manufacturers should "offer vehicle owners choices regarding the collection, use, sharing, retention, and deconstruction of data, including geolocation,[48] biometric, and driver behavior data that could be

---

[41] Federal Trade Commission, *supra* note 38, at 7.

[42] *Id.*

[43] RAND, *supra* note 4, at 94. *See also* Gillespie, *supra* note 19.

[44] Federal Trade Commission, *supra* note 38.

[45] Consumers want the ability to "use a personal smartphone to obtain data for navigation, to have email read aloud to the driver, to send SMS (text) messages by voice, and to have text messages read back aloud for the driver." Having all of this information stored in a vehicle shows how sensitive this data could be. *See* RAND, *supra* note 4, at 82.

[46] Federal Trade Commission, *supra* note 38, at 8.

[47] *Id.*

[48] *Geolocation*, TECHOPEDIA, https://www.techopedia.com/definition/1935/geolocation (last visited Feb. 22,

reasonably linked to them personally (i.e., personal data)."[49] A consumer's choice as to how their driving data may be shared is especially relevant to self-driving vehicles because many third parties will be interested in the data.[50]

3. Access/Participation

The third FIP is that consumers should have the "ability both to access data about him or herself—i.e., to view the data in an entity's files—and to contest that data's accuracy and completeness."[51] This particular FIP is important for self-driving vehicles because consumers should have access to the information their vehicle is collecting about them. Consumers may want to view what particular types of information are being gathered by the vehicle to better inform their decision as to whether they want the manufacturer to have control over their data or not. Furthermore, the FTC addresses access and participation to make sure consumers can correct data that is obtained from them.[52] In regards to self-driving vehicles, however, access and participation should be viewed in a light that reflects the importance of a consumer's knowledge of the nature of the information gathered from them. It is only through this light that consumers can make informed decisions about whether they want the data retained from them or not.

2017) ("Geolocation is the process of finding, determining and providing the exact location of a computer, networking device, or equipment. It enables device location based on geographical coordinates and measurements."). In the self-driving vehicle scenario, the consumer should have a choice as to whether the manufacturer has the ability to tell exactly where the consumer's vehicle is at all times based on geographical information taken from the vehicles Global Positioning System ("GPS").

[49] U.S. Department of Transportation, *supra* note 21, at 19.

[50] RAND, *supra* note 4, at 94 (stating that "insurance companies would be interested in individual driving habits," "retailers would be very interested in attracting motorists to their locations," and "law enforcement agencies [would] have considerable interest in using such data").

[51] Federal Trade Commission, *supra* note 38, at 9.

[52] *Id.*

4. Integrity/Security

The fourth FIP is "that data be accurate and secure."[53] The FTC promulgates that to "assure data integrity," data "collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form."[54] This definition is important because it draws attention to the protection of data from hackers; however it only speaks to information and does not address the issue of security in regards to the software components of the vehicle and the vehicle's operating system.[55] The Federal Automated Vehicles Policy suggests that the manufacturers should take it upon themselves to ensure that they "follow a robust product development process" that is designed to detect and adapt to cybersecurity threats.[56] While precedent exists regarding the protection of data within the vehicle, there is no established standard for the quality of a vehicles' cybersecurity against infiltration.[57]

5. Enforcement/Redress

The final FIP is enforcement and redress.[58] This particular FIP is important because without a means of enforcement, the other FIPs would be worthless.[59] The FTC states that there are different ways for the FIPs to be enforced.[60] The industry could self-regulate, "legislation [could] create private remedies for consumers,"[61] or there could be "regulatory schemes enforceable

---

[53] *Id.* at 10.
[54] *Id.*
[55] *Id.*
[56] U.S. Department of Transportation, *supra* note 21, at 21.
[57] *Id.* (telling industry participants that they "should consider and incorporate guidance, best practices, and design principles published by National Institute for Standard and Technology (NIST), NHTSA, SAE International, the Alliance of Automobile Manufacturers, the Association of Global Automakers, the Automotive Information Sharing and Analysis Center (ISAC) and other relevant organizations").
[58] Federal Trade Commission, *supra* note 38, at 10.
[59] *Id.*
[60] *Id.*
[61] *Id.*

through civil and criminal sanctions." [62] Enforcement is an interesting issue in the current self-driving vehicle industry because manufacturers are currently regulating their own vehicle standards with little to no oversight by any level of government.[63] The FTC recognizes that government enforcement is an option for regulating the implementation of the FIPs and this is reflected in the SPY Car Act.[64]

B. Federal Trade Commission Act

In response to an increased demand for regulation of unfair and deceptive business practices,[65] the United States Congress enacted the Federal Trade Commission Act ("FTCA").[66] The FTC receives its regulatory power from Section 5 of the FTCA,[67] which allows the FTC to "prevent" businesses "from using unfair methods of

---

[62] *Id.*

[63] Very few states have enacted some form of legislation to address the issues of self-driving vehicles. Most states that have passed legislation deal with the problem of defining a self-driving vehicle and authorizing this type of vehicle to be operated on the roads within the states. *See* U.S. Department of Transportation, *supra* note 21, at 41–52; *see also*, Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx (last visited Mar. 4, 2017) (showing a constantly updated list of every state that has passed legislation and every state with proposed legislation regarding self-driving vehicles).

[64] Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. 10 (2015) ("Enforcement—A violation of this section shall be treated as an unfair and deceptive act or practice in violation of a rule prescribed under section 18(a)(1)(B).").

[65] *See* Daniel J. Solove, *A Brief History of Information Privacy Law*, PROSKUER ON PRIVACY, PLI (2006) (providing an in-depth history of the evolution of privacy law and how the FTCA emerged based on the need to regulate unfair and deceptive business practices).

[66] *See* 15 U.S.C. § 41-58 (2012). *See also* Jeffrey H. Liebling, *Judicial Usurpation of the F.T.C.'s Authority: A Return to the Rule of Reason,* 30 J. MARSHALL L. REV. 283, 286 (1996) (explaining how "[t]he primary objective of the F.T.C. Act was to create an administrative body with broad regulatory authority to determine what business practices constituted unfair methods of competition").

[67] 15 U.S.C. § 45 is referred to as Section 5 of the FTCA because the FTCA starts at § 41 making § 45 the fifth section.

competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[68] The ability to prevent businesses from committing unfair and deceptive practices is solely a reactive authority and does not give the FTC the power to issue statutory regulations.[69] The SPY Car Act, however, would give the FTC the authority to issue regulations under the FTCA pertaining to privacy standards and would make a violation of these standards an "unfair and deceptive act or practice" under the FTCA.[70] This dual authority given to the FTC authorizes the FTC to assume a role it historically has not embraced.[71] Part IV will analyze how this dual authority gives the FTC the power it needs to effectively regulate the privacy standards for self-driving vehicles.

1. The FTC's Authority Under Section 5 of the FTCA

If the FTC determines that a manufacturer has been deceptive or has used unfair business practices, the FTC can bring an enforcement action through filing a lawsuit in federal court.[72] The FTC, however, conducts the majority of their regulatory power outside the purviews of the courts.[73] In its role as a regulatory

---

[68] 15 U.S.C. § 45(a)(2) (2012).

[69] The FTCA gives the FTC the authority to issue complaints against a company who has violated its privacy policies. *Id.* The FTCA, however, does not give the FTC the power to issue statutory regulations to which the companies must conform their privacy practices. *See id.* at § 45(b).

[70] The SPY Car Act states that the FTC will have the power to "prescribe regulations . . . to carry out section 27" of the FTCA. Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. 10 (2015).

[71] *See* Solove, *supra* note 65, at 39 (stating that the FTC, since 1998, has been "bring[ing] civil actions and seek[ing] injunctive remedies").

[72] *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FEDERAL TRADE COMMISSION https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited March 4, 2017) [hereinafter *Federal Trade Commission: A Brief Overview*].

[73] *Id.* Typically the only time companies refuse to settle and take the FTC to court is when the company believes the FTC has overstepped the scope of its statutory authority under Section 5 of the FTCA. *See also* Spencer Weber Waller, *Prosecution By Regulation: The Changing Nature of Antitrust Enforcement*, 77 OR. L. REV. 1383, 1394–95 (1998) (explaining how the courts have mostly taken on a "symbolic role" in overseeing the FTC in their

agency, the FTC monitors the marketplace and responds to complaints by initiating investigations, and if warranted, issues a complaint "setting forth its charges."[74] If the accused company continues to engage in the unlawful business practices or decides to contest the charges against them, the complaint is adjudicated and "a United States court of appeals may then enforce, modify or discharge the F.T.C. ruling."[75] It is difficult, however, for a company to successfully challenge the FTC's determination that the activity the company engaged in was unfair or deceptive. If the FTC's findings are "supported by substantial evidence," the court should dismiss the challenge in favor of the FTC "even if the finding is at variance with the position the court would have taken."[76] In other words, courts will not overturn a finding of "unfair or deceptive" as long as the FTC has substantial evidence to support their claim.[77] If a company charged with violation of Section 5 of the FTCA wants to challenge the finding by the FTC, the company will usually challenge the FTC's scope of authority under the FTCA.[78] This is important because self-driving vehicle

---

regulatory capacity and that the law "is determined in accordance with internal guidelines rather than case law").

[74] 15 U.S.C. § 45(b) (2006). *See also What We Do*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/about-ftc/what-we-do (last visited Feb. 23, 2017) ("We [the FTC] conduct investigations, sue companies and people that violate the law, develop rules to ensure a vibrant marketplace, and educate consumers and businesses about their rights and responsibilities."). *See also* Federal Trade Commission: A Brief Overview, *supra* note 72.

[75] Liebling, *supra* note 66, at 295.

[76] *Id.* at 295–96 (citing Litton Industries, Inc. v. F.T.C., 676 F.2d 364, 368–69 (9th Cir. 1982)).

[77] *Id.* at 294–96.

[78] The key word is "wants" to challenge the FTC. Companies will settle with the FTC out of court the majority of the time. *See Enforcing Privacy Promises*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited March 4, 2017) (showing how many companies have settled with the FTC in the recent past). If a company does, however, want to challenge the finding of the FTC, the form of the challenge will typically look like the defenses raised in cases such as: LabMD, Inc. v. F.T.C., 776 F.3d 1275 (2015) (LabMD claiming the FTC exceeded their statutory authority; 11th Circuit ruled in LabMD's favor); F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (2015) (determining whether the FTC had authority to regulate cybersecurity under the unfairness

manufacturers will be faced with complaints by the FTC if they breach their cybersecurity and data privacy standards as evidenced by the fact that the SPY Car Act makes a violation of the privacy standards a violation of the FTCA.

2. Application of the FTC's Section 5 Authority to Self-Driving Vehicles

The FTC's ability to effectively determine what is an unfair or deceptive business practice is both developed by the FTC and tested in the federal courts. The unfairness prong, however, versus the deceptive prong, is currently the subject of controversy.[79] The FTC typically pursues what they have determined to be a breach of cybersecurity under the unfairness prong while pursuing the breach of a commitment to a stated privacy policy under the deceptive prong.[80] Therefore, if Congress is going to include the FTC in the rulemaking process for cybersecurity and privacy standards in self-driving vehicles then it may need to revisit the issue of the FTC's authority under the FTCA, particularly for cybersecurity.[81] Effective regulation of these self-driving vehicles will require the FTC to monitor the companies manufacturing these vehicles to assure that they are complying with their stated privacy policies

---

prong of Section 5 of the FTCA; ruled in favor of the FTC thereby expanding its scope of authority under the FTCA to regulate cybersecurity). The trend of the judiciary in FTC authority case decisions dates all the way back to the 1920s when the U.S. Supreme Court was first faced with this authority question. The Court issued a very strict interpretation of the FTC's ability to determine what is unfair and deceptive in F.T.C. v. Gratz, 253 U.S. 421 (1920). However, the Court methodically chipped away at this ruling and broadened the FTC's authority until the 1980s where the Court once again ruled to restrict the scope of the FTC's authority. Liebling's article argues the courts are restricting the original intention of Congress in the FTCA and that the courts should look to once again broadening the FTC's authority and allowing them to act like the regulatory agency they were designed to be. *See* Liebling, *supra* note 66, at 296-313.

[79] *See* Liebling, *supra* note 66, at 296–313. (discussing challenges to FTC authority and how all of these recent challenges have come after the FTC has tried to prosecute breach of cybersecurity standards under the unfairness prong of the FTCA).

[80] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 627–48 (2014).

[81] *See* Liebling, *supra* note 66, at 313–18.

and not allowing consumers data to be stolen. Without clarity about the FTC's ability to regulate self-driving vehicle manufacturers under Section 5, the consumer is ultimately the one who suffers because of the lack of oversight for manufacturers and their practices.

The FTC, while not a rulemaking agency, has the ability to play an important role in the regulation of self-driving vehicle technology. The Senate included the FTC in the SPY Car Act to help the NHTSA create effective regulations. In order to do so, the NHTSA must account for the FIPs and the FTC's own regulatory authority under the FTCA.

III. THE SPY CAR ACT OF 2015

Self-driving vehicles have created a unique problem for the federal government because the U.S. Department of Transportation has never encountered a technology with such a high degree of autonomy. Since its inception "the U.S. Department of Transportation ("DOT") has been committed to saving lives and improving safety and efficiency in every way Americans move . . . ."[82] This regulatory effort includes automobiles, which are "on the cusp of a technological transformation."[83] As discussed previously, the current regulations on standard automobiles will not be adequate for the future regulation of self-driving vehicles.[84]

The primary objective of the SPY Car Act is "[t]o protect consumers from security and privacy threats to their motor vehicles, and for other purposes."[85] This will be achieved by amending the current Title 49 powers of the DOT, NHTSA, and FTC to regulate these self-driving vehicles.[86] The SPY Car Act is organized in a way that will amend the definitions section under 49 U.S.C. § 30102 to include crucial definitions that pertain to self-driving cars.[87] The SPY Car Act then breaks the issues into three

[82] U.S. Department of Transportation, *supra* note 21, at 5.
[83] *Id.*
[84] *See* RAND, *supra* note 4.
[85] SPY Car Act, *supra* note 8, at 1.
[86] *See id.*; 49 U.S.C. § 301 (1998).
[87] *See* SPY Car Act, *supra* note 8, at 2–3 (defining "Administrator" as the Administrator of the NHTSA; "Commission" as the FTC; "'critical software

categories: cybersecurity, [88] cyber dashboard, [89] and privacy standards.[90] This section details the SPY Car Act's categories and explains these sections' importance and purpose.

A. Cybersecurity Standards

The SPY Car Act's first main section is "Cybersecurity standards."[91] The cybersecurity section starts off by making a definitive statement that "[a]ll motor vehicles manufactured for sale in the United States . . . shall comply with the cybersecurity standards set forth" in this section.[92] The cybersecurity standards with which these vehicles must comply consist of three separate components: "protection against hacking,"[93] "security of collected information," [94] and "detection, reporting, and responding to hacking."[95] In addition to stating specific standards to which these vehicles must comply, the cybersecurity standards section also

---

systems' means software systems that can affect the driver's control of the vehicle movement"; "'driving data' include, but are not limited to, any electronic information collected about—(A) a vehicle's status, including, but not limited to, its location or speed; and (B) any owner, lessee, driver, or passenger of a vehicle"; "'entry points' include, but are not limited to, means by which – (A) driving data may be accessed, directly or indirectly; or (B) control signals may be sent or received either wirelessly or through wired connections"; and "'hacking' means the unauthorized access to electronic controls or driving data, either wirelessly or through wired connections").

[88] *Id.* at 3.

[89] *Id.* at 6.

[90] *Id.* at 8.

[91] *Id.* at 3. As mentioned in the introduction, it is beyond the scope of this Recent Development to analyze the cybersecurity standards portion of the SPY Car Act from a technical perspective. However, it is worthwhile to touch on what is said about cybersecurity standards within the SPY Car Act. The cybersecurity portion of the SPY Car Act is a deep enough issue to warrant its own recent development. The area of cybersecurity law is a very murky area of the law and is still in the process of developing and evolving to meet the needs of a rapidly changing technology industry.

[92] *Id.*

[93] SPY Car Act, *supra* note 8, at 3–4.

[94] *Id.* at 4–5.

[95] *Id.* at 5.

calls for "penalties" of "not more than $5,000 for each violation" of these regulations.[96]

The SPY Car Act gives the primary rulemaking authority for cybersecurity standards to the NHTSA after consultation with the FTC.[97] It is this relationship between the NHTSA and the FTC that makes the analysis of whether the SPY Car Act conforms to the FTC's reliance on the FIPs so important. These regulations in the SPY Car Act do not necessarily inform the industry participants as to the specific standards to which these cybersecurity measures must comply. Rather, the SPY Car Act only specifies that each manufactured vehicle must have some sort of protection against hacking, and the vehicle must have measures to prevent unauthorized access to the vehicle.[98]

B. Cyber Dashboard

The SPY Car Act's "Cyber Dashboard" is a means of giving notice to consumers of self-driving vehicles.[99] A cyber dashboard is a privacy policy notice affixed to the self-driving vehicle.[100] The features of the cyber dashboard must "inform consumers, through an easy-to-understand, standardized graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers."[101] The cyber dashboard must contain provisions "beyond the minimum requirements set forth in" the cybersecurity portion of the SPY Car Act and it must go beyond the requirements set forth "in section 27 of the Federal Trade Commission Act."[102]

This language contained in the SPY Car Act concerning notice does not entirely entail the requirements promulgated in the FIPs.[103] Although the cyber dashboard does effectively give notice as to how the vehicle will protect the privacy of the consumer, it

---

[96] *Id.*
[97] *See id.* at 3–6.
[98] *See id.*
[99] SPY Car Act, *supra* note 8, at 7.
[100] *Id.* at 6–7.
[101] *Id.* at 7.
[102] *Id.*
[103] *See id.* at 7–8.

does not address the issues of consent, consumer access, or third party access.[104] While these issues are discussed in the Privacy Standards portion of the SPY Car Act,[105] the U.S. Senate should look to including these requirements in the initial notice, the cyber dashboard, so that consumers can be fully informed as to how their data is being used and the rights the consumer has to this disposition of their data.

C. Privacy Standards for Motor Vehicles

The final portion of the SPY Car Act concerns "Privacy Standards for Motor Vehicles."[106] The purpose of this portion of the SPY Car Act is not only to give the FTC the power to regulate privacy standards and to issue statutory rules on privacy standards, but also to provide a framework for privacy standards to which self-driving vehicle manufacturers may be held. These standards incorporate the FIPs by using "transparency," "consumer control," and "limitations on use of personal driving information."[107] The SPY Car Act defines "transparency" as the "vehicle [providing] clear and conspicuous notice, in clear and plain language, to the owners or lessees of such vehicle of the collection, transmission, retention, and use of driving data collected from such motor vehicle."[108] The SPY Car Act defines "consumer control" as the ability of the consumer to opt-out of "the collection and retention of driving data" without losing "access to navigation tools or other features or capabilities, to the extent technically possible."[109] The SPY Car Act also states that a "manufacturer (including an original equipment manufacturer) may not use any information collected by a motor vehicle for advertising or marketing purposes without the affirmative express consent by the owner or lessee" unless provided with the owner's consent.[110]

---

[104] *See id.* at 7.
[105] *See* SPY Car Act, *supra* note 8, at 8–11.
[106] *Id.* at 8.
[107] *Id.* at 8–11.
[108] *Id.* at 8.
[109] *Id.* at 8–9.
[110] *Id.* at 9–10.

These provisions within the SPY Car Act accurately reflect the FIPs by requiring self-driving vehicle manufacturers to take the necessary steps to fully inform the consumer as to how their data is being used and giving the consumer control over their data.[111] These provisions are crucial for the effective regulation of self-driving vehicles because they allow a consumer to dictate how their data can be used.

Overall, the language of the SPY Car Act produces regulations that will effectuate the necessary regulation of self-driving vehicles. The SPY Car Act's most valuable tool is that it sets a solid groundwork that the NHTSA and the FTC can use to further promulgate rules. The next part further analyzes the provisions of the SPY Car Act and determines whether they are adequate as compared to existing privacy standards.

IV. WILL THE SPY CAR ACT HELP RESOLVE THE LEGAL ISSUES SURROUNDING PRIVACY IN A SELF-DRIVING CAR?

With so much talk about the concerns surrounding vehicle cybersecurity and privacy, the question now becomes, will the SPY Car Act help to alleviate these concerns? The purpose of the SPY Car Act is not only to provide rules and regulations for self-driving vehicles, but also to allocate rule-making authority to the NHTSA in conjunction with the FTC.[112] It is through this lens that the analysis of the provisions of the SPY Car Act will take place. While there may be portions of the SPY Car Act that could use some bolstering, the NHTSA and the FTC have the opportunity to compensate for any shortcomings by continuing to analyze the needs of the industry and consumers and reflecting that in the final rules published by both entities. Subsection A will analyze the cyber dashboard, notice requirements, and transparency against the FIPs and will argue for more transparency in the initial notice requirement. Subsection B will analyze the limitations on the use of driving data by manufacturers and how the requirements align with the current practices within the self-driving vehicle industry. Subsection C will scrutinize the authority given to the FTC through

[111] *See* SPY Car Act, *supra* note 8, at 8–11.
[112] *Id.* at 5–11.

the SPY Car Act to regulate privacy practices and how this aligns with the current ability of the FTC to regulate the industry. Subsection D will analyze the statutory rulemaking process that the FTC will be required to use and whether that process will be adequate in obtaining valuable input from consumers. Subsection E will address the lack of private remedies associated with companies' breach of their policy agreements and how the SPY Car Act has addressed this issue.

A. Notice and Transparency

The "cyber dashboard," or an affixed notice on the vehicle, and the notice requirement contained in the privacy standards, are effective regulations contained within the SPY Car Act.[113] The Federal Automated Vehicles Policy suggests a notice requirement,[114] and the FTC requires notice be given to consumers.[115] Thus, the SPY Car Act's requirement for manufacturers to give their customers notice is a step in the right direction. The notice requirement also will likely meet FTC standards because of the additional requirements of transparency, control, and limitations on the use, collection, and retention of the personal data.[116] These requirements are consistent with the FIPs and should be effective in stemming some of the concerns over data privacy within these vehicles.

There is an argument to be made, however, that notice of a manufacturer's privacy practices will not be effective enough to ensure that consumers are fully informed about companies' practices and the level of protection of the data.[117] Tesla's Customer Privacy Policy is a great example of a privacy notice given to consumers of self-driving vehicles.[118] While it can be

---

[113] *Id.* at 6–8.

[114] U.S. Department of Transportation, *supra* note 21, at 19.

[115] Federal Trade Commission, *supra* note 38, at 7.

[116] SPY Car Act, *supra* note 8, at 8–11.

[117] *See generally* Paula J. Bruening & Mary J. Culnan, *Through a Glass Darkly: From Privacy Notices to Effective Transparency*, 17 N.C. J. L. & TECH. 515 (2016).

[118] Tesla, Legal: Customer Privacy Policy, https://www.tesla.com/about/legal (last visited Feb. 24, 2017).

argued that Tesla should be lauded for its detailed privacy notice, it is unlikely that the average consumer will understand the lengthy legal document.[119] The SPY Car Act requires that "easy-to-understand"[120] language be used in the cyber dashboard feature and that consumers should be given "clear and conspicuous notice."[121] This provision will force manufacturers to trim down the complicated language and will help consumers better understand the privacy implications of self-driving vehicles.

The FTC will need to closely monitor privacy policies to ensure that the industry is conforming to the standards contained in the SPY Car Act. The SPY Car Act incorporates the FIPs by requiring straightforward language in privacy notices and those requirements will, in theory, diminish the amount of complicated language consumers will be forced to read. In reality, however, this regularly will not be the case because manufacturers have an interest in covering all aspects of legality and liability, which results in overly technical and detailed privacy notices.[122] Therefore, the FTC needs to take this into account in their proposal for rulemaking for privacy standards. In addition to the FTC's ability to intervene when a company has not complied with its own stated privacy policy,[123] the FTC must safeguard consumers from convoluted privacy notices by enforcing the cyber dashboard and privacy provisions laid out in the SPY Car Act.

---

[119] *See id.* ("Telematics log data: To improve our vehicles and services for you, we may collect certain telematics data regarding the performance, usage, operation, and condition of your Tesla vehicle, including the following: e.g., vehicle identification number; speed information; odometer readings; battery use management information; battery charging history; electrical system functions; software version information; infotainment system data; safety-related data and camera images.") This lengthy description covers only one facet of the information Tesla retains. The average consumer probably would not notice that information regarding your "infotainment" is collected. *See also* Bruening & Culnan, *supra* note 117, at 526–29.

[120] SPY Car Act, *supra* note 8, at 7.

[121] *Id.* at 8.

[122] Bruening & Culnan, *supra* note 117, at 543.

[123] Solove, *supra* note 65, at 39.

B. Limitations on Use of Driving Data

Another regulation that would create a solid foundation from which the NHTSA and FTC could work is the limitation on the use of the collected driving data.[124] With constant Internet connection, Internet Service Providers ("ISPs") like Verizon, AT&T, IBM, and Google will have access to the personal data generated by self-driving vehicles.[125] These ISPs will provide the Internet broadband on which self-driving vehicle technology will rely,[126] thus introducing yet another party who has access to the information gathered from the vehicle and transmitted over broadband. While the SPY Car Act regulations may limit the manufacturer's use of data, there is an open question as to what choices a consumer has regarding the information retained by ISPs. Although the SPY Car Act does not speak directly to this question, the FTC does have advisory authority and should seek to apply the FIPs to all parties involved in self-driving vehicle operation.[127]

While this may seem like a vulnerability, the SPY Car Act shows that it is aware of the concern over secondary uses of personal information.[128] The language included in the SPY Car Act limiting a manufacturer's use of personal driving data has the regulations moving in the right direction.[129] While Congress does

---

[124] SPY Car Act, *supra* note 8, at 9–10.

[125] *See* RAND, *supra* note 4, at 158 (stating how self-driving vehicle "security needs to be in the 'cloud'" and noting that "only a cloud-based solution could manage all of the media and data involved in" a self-driving vehicle).

[126] *See id.* at 82 (explaining that in order for self-driving vehicles to operate effectively on a horizontal communications platform there needs to be 3 components that work together: "(1) the car, (2) the technology brought into the car, and (3) the Internet 'cloud'").

[127] The FTC states that "choice relates to secondary uses of information—*i.e.*, uses beyond those necessary to complete the contemplated transaction." The FTC also states that one secondary use of this information could be "transfer of information to third parties." *See* Federal Trade Commission, *supra* note 38, at 8.

[128] *See* SPY Car Act, *supra* note 8, at 8–10. This is evidenced by the fact that the SPY Car Act includes language giving the consumer control over the "collection and retention of driving data" and the fact that the SPY Car Act also limits manufacturers as to what they can do with the data without express consent from the consumer.

[129] *See id.*

effectively establish limitations on use of information by the manufacturer, Congress should seek to include strong language in the SPY Car Act that gives the FTC authority to govern information sharing with every potential party involved in the operation of a self-driving vehicle.[130] That the SPY Car Act does not address the idea that an Internet medium may have access to consumer information shows the need for additional language consistent with the choice/consent FIP where the consumer has the option to restrict information access to all parties.[131]

The privacy policy used by Tesla gives some insight in to how current manufacturers are addressing information sharing.[132] Tesla's privacy policy aligns with the provisions of the SPY Car Act in that it says that they "do not share information that personally identifies you [the consumer] with unaffiliated third parties for their marketing purposes unless you [the consumer] opt in to that sharing."[133] This language is consistent with the limitations imposed by the SPY Car Act.[134] The FTC, however, uses stronger language in the FIPs that suggests manufacturers, or any company retaining consumer information, should not share any consumer information to any secondary entity without consent from the consumer.[135] It may not be feasible, as self-driving

[130] *See* SPY Car Act, *supra* note 8. The FTC, through its rulemaking capacity under the SPY Car Act, needs to work with consumers and the industry so they can anticipate what these "secondary uses" could take the form of. This may come to light as self-driving vehicle technologies become more sophisticated, however, the FTC should strive to identify potential additional entities that may need governance.

[131] *See* Federal Trade Commission, *supra* note 38, at 8.

[132] Tesla, *supra* note 118.

[133] *Id.*

[134] SPY Car Act, *supra* note 8, at 9.

[135] Federal Trade Commission, *supra* note 38, at 8–9 (explaining how "secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as transfer of information to third parties"). The FTC also speaks to a system of allowing consumers to "opt-in" or "opt-out" of having their data retained with the ability of the consumer to specifically "tailor the nature of the information they reveal and the uses to which it will be put." *Id.* The FTC also states that in the online realm, choice can be easily "exercised by simply

technology is new and evolving, to completely restrict manufacturers such as Tesla from sharing information about their drivers.[136] Tesla's privacy policy, however, includes provisions that appear vague and would leave a consumer wondering with whom their data is being shared.[137] Because of these vague terms contained in privacy policies coupled with the need for manufacturers to have the ability to data share, the FTC, through its rulemaking authority needs to strive to create a data sharing system that works for both consumers and manufacturers. Taking into account the FIPs and the Federal Autonomous Vehicle Policy Guidance, the FTC should create a system where the consumer can specifically tailor the data they wish to be shared and manufacturers are required to de-identify the data even when shared with other parties.[138]

C. Enforcement Authority Given to the FTC Under the FTCA

The SPY Car Act gives the FTC primary rulemaking authority for privacy standards and makes a violation of the privacy standards "an unfair and deceptive act or practice" under the FTCA.[139] Giving this type of dual authority provides the FTC with the requisite tools to effectively regulate the privacy standards in self-driving vehicles. This provision of the SPY Car Act is

---

clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected." *Id.*

[136] *See* U.S. Department of Transportation, *supra* note 21, at 18 (suggesting a system of anonymous data sharing that would promote "data sharing to enhance and extend safety benefits . . . [s]uch shared data would help to accelerate knowledge and understanding of HAV performance, and could be used to enhance the safety of HAV [self-driving vehicle] systems and to establish consumer confidence in [self-driving vehicle technologies]").

[137] *See* Tesla, *supra* note 118 (stating that Tesla "may share information with our service providers and business partners when necessary to perform services on our or on your behalf" with no mention of whether you have control over these disclosures"). Tesla also lays out a list of "third party service providers and channel partners" with whom they may share information. *Id.* Tesla does give an opt-in option for certain types of third parties, however, Tesla also includes language that could lead a consumer to believe they have no choice as to whether their information is shared with certain types of entities.

[138] *See supra* note 135.

[139] SPY Car Act, *supra* note 8, at 10.

important because it eradicates any ambiguity as to whether privacy violations will fall under the current FTC authority within the FTCA. As discussed in Part II,[140] the FTC has relied on case law to shape the scope of its authority to regulate cybersecurity and privacy standards.[141] By explicitly stating that the FTC can prosecute a violation, Congress has given the FTC the power it needs to operate as a federal enforcement agency as Congress originally intended.[142]

D. A Clear Avenue for Industry Input

Another area of concern surrounding the SPY Car Act is the tension it may generate between the industry participants and the power of regulation created in the NHTSA and the FTC. This tension can be seen in other types of industries, such as the current vehicle industry, and the self-driving vehicle industry should not, theoretically, have much of a problem with government oversight.[143] The SPY Car Act refers to industry "best security practices" and addresses how the self-driving vehicle industry should use these best practices to test the cybersecurity of the vehicle.[144] Because the technology is still new and relatively untested, the federal government will need to collaborate with the industry so the regulations reflect the actual best practices of the industry and the safest measures for the consumer.

The SPY Car Act initiates this public collaboration by requiring the FTC to issue regulations "in accordance with section 553 of title 5, United States Code."[145] This particular rulemaking statute would require the FTC to publish a notice of proposed rule making in the Federal Register, and the notice must include

---

[140] *See supra* note 65 and accompanying text.

[141] Regulation of cybersecurity under the unfairness prong is the prong that is being challenged more often. Regulation of privacy standards under the deceptive prong is relatively settled, and most companies charged with a violation of their privacy policy will typically settle with the FTC and pay civil penalties. *See supra* note 78.

[142] *See* Liebling, *supra* note 66, at 283.

[143] *See* RAND, *supra* note 4, at XXII.

[144] SPY Car Act, *supra* note 8, at 4.

[145] *Id*. at 10–11; 5 U.S.C. § 553 (2012).

logistical details for public hearings on the rule, the "legal authority" proposing the rule, and the subject matter covered by the rule.[146] These statutory requirements will give the FTC an opportunity to interact with the industry participants and obtain valuable information from them, which, in turn, will improve the quality of final regulations published by the FTC.[147] Strictly following the statutory guidelines, however, may not be enough to illicit adequate input from the average consumer interested in owning a self-driving vehicle.[148]

An effective way to obtain industry and consumer input on privacy regulations is, in addition to following the statutory requirements laid out in 5 U.S.C. § 553, to create a webpage under the FTC and NHTSA government websites so consumers and industry players can comment on what seems to work and what does not work for privacy regulations. This webpage could be updated with proposals from the FTC and NHTSA and allow comments on those particular proposals before implementing them. The prevalence of self-driving vehicles is evidence that society is becoming increasingly technologically advanced.[149] Therefore, the FTC should use a more technologically advanced solution for obtaining valuable input from consumers such as a website or social media postings about proposals and rules.

E. Lack of Redress for Consumers

One staggering deficiency in the SPY Car Act is the lack of redress for consumers. The FIPs speak to the importance of redress and how there are multiple ways to seek redress and enforcement

---

[146] 5 U.S.C. § 553(b).

[147] U.S. Department of Transportation, *supra* note 21, at 49–50. Although the U.S. DOT is analyzing NHTSA rulemaking the analysis is the same for the proposed rulemaking for the FTC under the SPY Car Act. The U.S. DOT states that "[r]ulemaking generally takes the longest . . . but it enables the Agency to make the broadest and most thorough changes to governing regulations, and gives the public the greatest opportunity to participate in the Agency's decision-making process." *Id.*

[148] *See generally* Richard Williams, *Regulation Checklist: Common Pitfalls in Regulations* (George Mason Univ., Working Paper No. 10-01, 2010).

[149] *See* Max Roser, *Technological Progress*, OUR WORLD IN DATA (2016), https://ourworldindata.org/technological-progress/.

for consumers could be established.[150] The most effective way to do so would be to establish "private rights of action for consumers harmed by an entity's unfair information practices."[151] The FTC states that creating private remedies for consumers there would provide "strong incentives for entities to adopt and implement" the FIPs and would "ensure compensation for individuals harmed by misuse of their personal information."[152] The specific form of these remedies would be something that would need to be expanded upon later; just adding redress language to the SPY Car Act could strengthen the self-driving vehicle industry and could lead to increased consumer comfort in buying a self-driving car.

A remedy for breach of the privacy standards, however, would fall under the powers of the FTC under the FTCA to "seek consumer redress from the" company who caused the injury to the consumer.[153] Therefore, it does not seem that it would be difficult to pursue redress on behalf of consumers who were injured by a self-driving vehicle manufacturer that has breached its privacy policy because that area of the FTC's authority is so settled. However, there may be an issue as to what types of redress would be associated with a breach of the vehicle's cybersecurity, which carries higher risk of injury. Even though the SPY Car Act does not address a specific remedy for consumers, by making a breach of the privacy standards an "unfair and deceptive act or practice" under the FTCA, Congress has effectively created a type of remedy for consumers operating through the FTC.[154]

V. CONCLUSION

The SPY Car Act is an effective first step in establishing industry standards for self-driving vehicle security and privacy. There are many questions left unanswered, and this intersection between technology and the law presents a unique challenge to lawmakers, industry participants, and consumers. The SPY Car

---

[150] *See* Federal Trade Commission, *supra* note 38, at 10–11.
[151] *Id.* at 11.
[152] *Id.*
[153] *See* Federal Trade Commission: A Brief Overview, *supra* note 72.
[154] *See* SPY Car Act, *supra* note 8, at 10.

Act does many things well, and due to the complete lack of existing regulations, the SPY Car Act creates the necessary avenue for the federal government to catch up to self-driving technology. Among the positive aspects of the SPY Car Act, it ensures that manufacturers abide by certain rules and regulations by attaching civil penalties to violations[155] and more closely follows the original FIPs promulgated by the FTC. The SPY Car Act also provides consumers with an avenue for redress against companies that violate their stated privacy policies. The high value of the information these self-driving vehicles will contain calls for a stringent system of governance over self-driving vehicle manufacturers, and by making a violation of the privacy standards contained in the SPY Car Act fall under the prosecutorial authority of the FTC, Congress has provided the FTC with the power it needs to govern this technology.

The SPY Car Act says that its purpose is to "protect consumers from security and privacy threats to their motor vehicles" and the SPY Car Act does make an adequate attempt to do this.[156] The SPY Car Act does many things well; nonetheless, Congress needs to address its negative attributes with expediency. The disconnect between the industry and those that seek to regulate the industry must be addressed. Without communication between key industry players and government regulators, these self-driving vehicles could create an insurmountable burden that could prevent the industry from ever crossing the starting line. The notice of proposed rulemaking is a very good tool the FTC can use to effectuate communication between the industry, government, and consumers. This notice of proposed rulemaking needs to be bolstered by a more technologically advanced method of commenting on proposed rules. By making the rulemaking process more user friendly, the FTC could illicit more helpful input from consumers, and a greater number of consumers would have an opportunity to have their voice heard.

Overall, the SPY Car Act has the potential to help standardize practices that desperately need cohesion. From consumers' rights

---

[155] *Id.* at 5, 10.
[156] SPY Car Act, *supra* note 8, at 1.

to the industry's business interests to the government's regulatory interests, the issue of self-driving vehicle technology is far from being resolved. It is going to take a concerted effort among consumers, the industry, and the government to create unassailable vehicles that are safe and protect consumer privacy. After all, the benefits of these vehicles have the potential to shape the future of transportation for the United States.