Global Positioning Systems and Social Media—Anathemas to Privacy

By: Basil A. DiSipio

Basil A. (Bill) DiSipio has been a member of the IADC since 2002 and is a former President of the IADC Foundation. Mr. DiSipio is the Managing Shareholder of Lavin, O'Neil, Cedrone & DiSipio. The firm maintains offices in Philadelphia, Pennsylvania, New Jersey, New York, New York and Rochester, New York. For close to 40 years, he has been a litigator and trial lawyer representing corporations, insurers, and non-profit and religious organizations in tort and commercial litigation. Mr. DiSipio was assisted in writing this article by a former Lavin, O'Neil, Cedrone & DiSipio law clerk, Caitlin Wilenchik. She is a 2016 graduate of The George Washington University School of Law.

LIKE a cat and mouse game, privacy law strives to keep up and provide redress for injuries related to information extracted from the latest technology. As a result of social media driven technology, society's notion of what should be protected personal information has changed over time.[1] Posting a picture of an intimate moment between two people has become commonplace, and so has meeting that person through a cellphone application. In an age where face-to-face interactions can be completely avoided, society's privacy concerns have adjusted, inspiring new law, but not implementing it. Courts are left to analyze new privacy issues using antiquated methods.

Juxtaposing old practices people used to unlawfully invade another's privacy to the new practices used reflects how old privacy law does not properly address the new problems. People are no longer breaking into buildings or homes to steal sensitive information. This world is now full of people who

[1] *See, e.g.*, 2 Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (opining about the negative implications of 'instantaneous photography' as an invention with new threatens to the invasion of privacy, a right protected by the U.S. Constitution and common law).

carry tremendous amounts of sensitive information in their cell phone, and someone no longer has to steal the cell phone to get that information. It can be accessed remotely. The cell phone has advanced to a degree greater than those devices used to send men to the moon. It does not help that because of the current legal landscape, it is unclear whether the average person has a right to protect a majority of the information supplied to social media applications or the unknown information collected.

A modern cell phone is now called a smartphone, which is capable of sharing its physical location at any time.[2] Smartphones have a Global Positioning System ("GPS") chip inside, and the chip uses satellite data to calculate a person's exact position, which is supplied to various social media applications.[3] Even if a GPS signal is unavailable, some social media applications, like Foursquare,[4] can use a less accurate method to gain information from cell towers to find someone's approximate position.[5] GPS and social media applications garner a mass amount of its user's private information, and this process poses a threat to their privacy because industries that manufacture this technology have unregulated security measures to protect sensitive information, if they have any measures at all.

Years ago, small children could gain access to their parents' computers, enter an AOL chat room and at most, risk knowingly sharing personal information with the wrong person. It started with chat rooms, then MySpace and LiveJournal where anyone could publish their thoughts, feelings, birthdays, identify family members and friends, and the website could, in turn, provide direct access to other users. Today, add Twitter, Tumbler, Instagram, Facebook and Snapchat to the social media category as applications available at all times on a cell phone, which provide a user with more outlets to project personal information to others and keep a permanent log of this information. These social media outlets can help someone create a

---

[2] *See also* Scott Webster, *Four Ways to Share Your Exact Location with Family (and Why)*, C NET (Feb. 9, 2016, 5:00 AM), https://www.cnet.com/news/location-tracking-apps/ (geo-specific applications used to track a user on a smartphone include those that are carrier-branded, but can also be downloaded intended to share with family and friends).

[3] Daniel Ionescu, *Geolocation 101: How It Works, the Apps, and Your Privacy*, PCWorld (Mar. 28, 2010, 7:45 PM), http://www.pcworld.com/article/192803/geolo.html.

[4] Foursquare, *About Us,* WWW.FOURSQUARE.COM, https://foursquare.com/about (Foursquare shares information with friends and has a game one can play with friends to share new places) (last visited September 4, 2017).

[5] *Id.*

brand; or keep family and friends abreast of their life by sharing images, opinions, and details; or create an easy opportunity for others to unlawfully gain or use personal information.

Social media applications succeed when users use them as much as possible. Profits increase the more information a customer shares, but this information can also be mined and traced by the wrong person. GPS information a company employee can acquire from a vehicle may or may not include the actual physical location of a vehicle, its previous locations manually entered into the navigation system, and the last location the vehicle was parked, also unknown to most consumers. As technology has advanced, so has the average criminal.

In addition to the information a user voluntarily shares, most social media applications use the location-based capability to increase functionality. When someone unlawfully gains private information, it is questionable whether the victim has redress against a company who was in charge of managing this information. Since the average user is not technologically advanced enough to understand how to secure it and social media is hard to avoid in the modern age, this leaves the company with more responsibility to protect consumers.

Though the United States once led the world in its innovative technology, so much of technology has changed since the 1970s that now privacy law requires reform.[6] The lack of reform is due in part over

[6] *See, e.g.*, European Union Regulation 2016/679 of the European Parliament and of the Council, *On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (Apr. 27, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. *See also,* Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Treaty No. 108 (1981), https://rm.coe.int/1680078b37. *But see,* The White House, *Administration Discussion Draft: Consumer Privacy Bill of Rights Act* (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (no

legislative debates about whether tailored legal reform will not serve a changing technical realm, but this argument may be waning. So, reform is timely. According to electrical engineer Gordon Moore, computer-processing speeds hit their limit once computers are as small as atomic particles.[7] This means that in five years, the central processing unit, or the 'brains' of a computer, may only experience incremental progress.[8] Both smart phones and computers contain central processing units. Both contain location-based technology and are the site where the majority of social media applications are accessed.

One industry facing a recent surge in technology is the automotive industry. This article primarily narrows in on this area of new growth, since automobiles create a unique set of privacy and liability concerns. There is no clear directive that guides manufacturers to protect private information. Both GPS and various social media applications can integrate with a car system and present active threats to its private information. The automobile is yet another device that contains a computing unit, except one that may need more protection. If a car's system is unlawfully accessed, not only could a lot more information may be seized, but the passenger could also lose immediate control of the vehicle's functionality. A national directive must protect what information society deems private, and outline an advanced policy that manufacturers must follow to keep information private. Current legislation does not directly punish or outline the duty a company has in this new technological world to prevent unlawful access to a customer's private information.

Part I of this Article addresses the conceptual relationship between the need to update privacy law and the policies behind developing it. Part II grounds this need to update current privacy law by using the newest advances in the automotive industry to describe how someone could hypothetically access data unlawfully and what harm this action could bring. Part III

---

progress on this bill as introduced during the last administration).

[7] Tom Simonite, *Moore's Law is Dead, Now What?* MIT TECH. REV. (May 13, 2016), https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/ (Moore's Law is the theory of continuously cramming more silicon resistors onto chips, which must reach its maximum. This theory was predicated off of Gordon Moore of Intel nearly fifty years ago, and Intel has recently suggested that microchips can only shrink for another five years.).

[8] Chris Green, *The End of Moore's Law? Why the Theory that Computer Processors will Double in Power Every Two Years May Be Becoming Obsolete*, INDEPENDENT (2015), http://www.independent.co.uk/life-style/gadgets-and-tech/news/the-end-of-moores-law-why-the-theory-that-computer-processors-will-double-in-power-every-two-years-10394659.html.

addresses current privacy laws that are outdated to deal with new technology, which opens the door to an unregulated market that leads to privacy concerns. Part IV discusses the latent concerns behind outdated regulations as applied to new technology, then suggests reasons why a more tailored approach to privacy law in light of new technology acknowledges the unease and better achieves the intended end, which is to address a security breach in private information using social media and location-based technology as a pathway.

I. Setting the Stage for Legislative Reform

Not too long ago, cars without seatbelts were the norm. Recognizing the societal cost of accident induced injuries, Congress enacted laws designed to ensure consumer safety. First, a federal law created an administration to mandate uniform safety standards for vehicles and encouraged states to police and address its citizen's safety.[9] Soon after, manufacturers began developing and producing vehicle safety features, and states also adopted and required manufacturers to comply with specific safety regulations.[10] Now, cars without seatbelts are obsolete.[11]

Privacy law originated from a case that spurred public outcry. In response, New York enacted a statute that acknowledged privacy as a right.[12] New York's response started a national trend, and many other states followed suit to enact legislation solidifying a citizen's right to keep some things private.[13] American common law provides a basis for privacy tort violations,

[9] *See* National Traffic and Motor Vehicle Safety Act of 1966 ([formerly] 15 U.S.C. § 1381 *et seq.*) (requiring automobile manufacturers to institute safety standards); Highway Safety Act, 23 U.S.C. § 402 (1966) ("Each State shall have a highway safety program approved by the Secretary, designed to reduce traffic accidents and deaths, injuries, and property damage resulting therefrom. Such programs shall be in accordance with uniform guidelines promulgated by the Secretary.").

[10] *See, e.g.*, Ins. Inst. for Safety Highway Loss Data Inst. (Feb. 2017), http://www.iihs.org/iihs/topics/laws/safetybeltuse?topicName=Safety%20belts#tableData (requiring Pennsylvania children under 18 to wear a seatbelt and providing fines as punishment for noncompliance). *See*, Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (1902) (creating public outcry over the court rejecting Brandeis and Warren's interpretation that a citizen had a right to privacy, specifically against appropriation of one's image in this case).

[11] *See* Wiley Act, Publ. L. No. 59-384, 34 Stat. 768 (1906), 21 U.S.C. § 1-15 (1934), *repealed by* 21 U.S.C. § 329(a) (1938) (making it unlawful for any person in the United States to manufacture any food or drug that is adulterated or misbranded).

[12] *Roberson*, 171 N.Y. 538, 64 N.E. 442 (1902).

[13] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 385 (1960), available at http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1.

which include the intrusion upon a person's seclusion or solitude, or into their private affairs; public disclosure of embarrassing private facts; publicity which places a person in a false light in the public eye; and appropriating one's name or likeness.[14]

There is no specific legislation that enforces measures to protect data security on the internet-of-things,[15] shorthand for the network of computing devices within different products that connect through the Internet. The threat of another person accessing global positioning data mined from social media applications is of main concern.[16] Specifically, there is no legislation or regulatory guidance that could provide designed security measures for companies that control devices and its data storage.

Federal regulations, historically a leader, fail to adequately protect consumers against the mishandling and misappropriating of their protected information. Potential harm from these actions comes in the form of mental and/or physical effects, and may frequently involve individuals in two different states. When an individual supplies information to their social media applications, a criminal can gain access to it and either harass or find the victim and cause harm.[17] Since the dawn of the Internet-of-Things, it is not difficult for criminals to gain a victim's exact location, their personal information, and even instantly exert control of their device.[18]

Privacy violations by or against public actors are clearly regulated and are not discussed in this article

---

[14] RESTATEMENT (SECOND) TORTS § 652 (Am. Law Inst. 1970).

[15] *Internet of Things, Privacy & Security In a Connected World*, FTC STAFF REPORT (Jan. 2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[16] *Id.* at 49 (The FTC ". . . has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach."). *See also*, Fed. Trade Comm'n, *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. On Commerce, Science & Transportation* (May 9, 2012) (statement of FTC), available at https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf.

[17] *See, e.g.*, Elonis v. United States, 135 S. Ct. 2001 (2015) (threatening his wife on Facebook upholding a subjective intent to threaten is needed as proof over the internet for a plaintiff to win a case under transmitting threats over interstate commerce).

[18] *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

to narrow its scope.[19] There are state statutes that punish private actors for accessing other devices and federal statutes that protect sensitive information supplied to certain industries like healthcare.[20] State statutes that address computers involve hacking or trespassing, but do not specifically mention the duty to prevent the use of private information garnered from another's device using advanced channels of the Internet-of-Things.[21] In other words, state or federal technical legislation does not address any company or manufacturer liability to a customer for a breach in security.

Companies find it helpful to foresee potential liability to consumers for a security failure, and there is nothing like the threat of litigation in terms of an incentive to follow any regulations to put them on notice of any liability. So far, the Federal Trade Commission ("FTC") has only one case that involved the Internet-of-Things. It outlines how important design-specific legislation could be to help provide guidance or else companies could face legal repercussions for neglecting to monitor data properly.

The FTC's Internet-of-Things case involved a company named TRENDnet.[22] TRENDnet marketed its Internet-connected cameras for purposes ranging from home security to baby monitoring, claiming they were "secure."[23] The FTC alleged that the company transmitted user login credentials over the Internet, then stored them on users' mobile devices, and failed to test consumers' privacy settings to ensure that the video feeds marked as "private" would stay private.[24] As a result of the company's failure to protect consumers, hackers were able to access live feeds from security cameras and conduct "unauthorized surveillance of infants sleeping in their cribs, young children playing,

---

[19] US CONST. AMEND. IV (granting citizens privacy against unreasonable searches from government actors); The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (punishing those who knowingly or intentionally access computer government files in various degrees of culpability).

[20] The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub. L. 104–191, 110 Stat. 1936, enacted Aug. 21, 1996).

[21] *See*, Nat'l Conf. of State Legislatures, *Computer Crime Statutes* (Dec. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (listing state laws making hacking and computer trespass unlawful, and two states make ransomware unlawful).

[22] Press Release, FTC, *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy* (Sept. 4, 2013), available at https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

[23] *Id.*

[24] Complaint of FTC, TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (consent), available at http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

and adults engaging in typical daily activities."[25] Devices have the capability to store highly sensitive information, and actors must be held accountable for failing to protect this information. The majority of consumers are entirely reliant on companies to protect them against harm, as most consumers are not educated on the intricacies of any technical device.

Opponents of Internet-of-Things security legislation are concerned it may stifle innovation, because the information Internet-of-Things devices collect makes each device more advanced.[26] Industries collect consumer data as a tool to improve their products' functionality by using the information supplied to the device to personalize their features to the customer's liking, or better direct advertising. Some consumers prefer this method, as a device can then direct specific data to him or her depending on their needs.[27] A person can search for flights to Philadelphia from Washington, D.C. on their computer or smartphone then leave the website, and find an advertisement on the next website for tours to visit the Liberty Bell, or for the flight discounted, or for hotels in Philadelphia. The next time they go to the website to book their flight, it may also remember their latest search and automatically fill in her name and address. But as people have become increasingly reliant on their personal devices, the line separating personal information one considers, knows, or expects to be private has become blurred.

Since industrial and informational products have merged to form a new hybrid in the automotive industry, the Internet-of-Things has increased its capacity to collect and share protected information. This new type of automobile poses a unique concern to consumers, and their privacy is at risk in an unregulated market. With GPS and social media connected to most cars and beginning with some homes which are both inherently private, hackers can facilitate multiple attacks on each device by accessing one device that contains security vulnerabilities. Recent developments that involve the

---

[25] *Id.* at 5.

[26] *See* FTC STAFF REPORT, *supra* note 15 (citing Comment of Internet Commerce Coal., #484 cmt. #00020 at 2) (remarking about concerns over the Federal Trade Commission regulating the internet-of-things too much which could stifle innovation). *But see id.* (citing Comment of Tech. Policy Program of the Mercatus Ctr., George Mason Univ., #484 cmt. #00024 at 1 and 9) (advising policymakers against addressing an issue that may be ripe or to "exercise restraint and avoid the impulse to regulate before serious harms are demonstrated").

[27] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf, (addressing new ways to consume and use big data, including data that is "born digital" like global positioning system data and website browsing).

merger between GPS and social media have only caused more concern over potential risks.

II. Various Opportunities for a Data Breach in New Automotive and Social Media Technology

There is no need to explain how dangerous it may be that someone else has the capability of taking control of your vehicle while you drive.[28] Now, there are an increasing number of non-native manufactured parts on the market that can connect to a vehicle and offer the opportunity for such a data breach.

First, vehicles contain more than 100 computer processors within them that breed complexity. Within the past few months alone, manufacturers like Ford, Hyundai, and BMW have announced their intent to integrate the Amazon Alexa[29] into their vehicles so that a user can remotely connect and share information with their home.[30] This "home-to-car" integration, for example, allows someone to unlock their car, start it, and manage its internal functionality all from inside the home. Ford's AppLink software, which would link to Amazon, is open-source software.[31] Open source means the software is non-proprietary, which allows users to modify the available original source code to potentially make security repairs or modify the vehicle's functionality entirely.[32]

BMW has integrated and encouraged car manufacturers to have open-source software to better

[28] Chrysler recalled 1.4 million vehicles after hackers demonstrated how they could remotely hack Jeeps and control their functionality. New techniques were administered to hack these same vehicles. *See* Andy Greenberg, *The Jeep Hackers are Back to Prove Hacking Can Get Much Worse*, THE WIRED, (Aug. 1, 2016), https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

[29] Amazon, *Why Alexa?*, WWW.AMAZON.COM, https://developer.amazon.com/alexa (last visited September 5, 2017)("Alexa is built in the cloud, so it is always getting smarter. The more customers use Alexa, the more she adapts to speech patterns, vocabulary, and personal preferences.").

[30] Kirsten Korosec, *Start Your Car from Inside Your Home Using Amazon's Alexa*, FORTUNE (Aug. 18, 2016), http://fortune.com/2016/08/18/hyundai-genesis-amazon/.

[31] *See,* Ford, *Alexa in the Car: Ford, Amazon to Provide Access to Shop, Search and Control Smart Home Features on the Road* (Jan. 4, 2017), https://media.ford.com/content/fordmedia/fna/us/en/news/2017/01/04/alexa-car-ford-amazon-shop-search-home.html.

[32] *See*, *History*, OPEN SOURCE INITIATIVE (last revised 2012), https://opensource.org/.

serve their consumers.[33] Groups like the Automotive Grade Linux Workgroup have collaborated with at least ten major automotive companies to promote an open-source project that encourages automakers, suppliers and technologies to collaborate and accept open software for connected cars. [34] However, security risks to the proprietary code are the primary reason some manufacturers, like Toyota, prefer closed software.[35] Data is valuable. The open-source software arguably allows, by a crowd-sourced peer-review process, one to discover source code defects, but it can also be susceptible to a less advanced crowd of reviews, which welcome security risks.

Recent technological advances in automobiles also consume and store even more information than ever before. BMW, for an example, has in-car sensors that can detect whether a child is in the vehicle. It is helpful to think of the car personified to understand how it manages its information. The car 'learns' it has a child in the car and can help increase its safety by 'communicating' with other vehicles on the road. The car may also share this information with other merchants in the area by accessing their devices so they can direct child-centric advertising to the parents in the car.[36] While sharing information, the car can also 'speak' to the passenger by consistently providing and storing information like directions and contacts from the passenger's phone to communicate

[33] *See* Alexandra Sage, *Toyota, BMW, and Allianz Ink-Sharing Deal with Autonomous Start-up Nauto*, REUTERS (Oct. 7, 2016), http://www.reuters.com/article/us-autonomous-nauto-idUSKCN1271FX (the proposed system integrated into BMW and Toyota vehicles would also deter a driver's bad behavior, compile congestion data, and other road conditions).

[34] *See generally* Automotive Grade Linux, *Announcements* (2017), https://www.automotivelinux.org/news/announcements.

[35] *See generally* Jim Zemlin, *The Next Battleground for Open Source is Your Car,* WIRED (Oct. 12, 2012, 9:30 AM), https://www.wired.com/2012/10/automakers-become-software-makers-the-next-battle-between-open-and-closed/.

[36] *But see,* Latanya Sweeney, *Discrimination in Online Ad Delivery* DATA PRIVACY LAB (Jan. 28, 2013), http://dataprivacylab.org/projects/onlineads/1071-1.pdf (explaining the downside to advertising can be that web searches involving black-identifying names (e.g., "Jermaine") were more likely to display ads with the word "arrest" in them than searches with white-identifying names (e.g., "Geoffrey"). This research was not able to determine exactly why a racially biased result occurred, recognizing that ad display is algorithmically generated based on a number of variables and decision processes.

and navigate.[37] Now, a car can also 'communicate' with the driver's home. All of a sudden, there is a lot more a car can do than just transport.

In the example above, the car was able to share information with a third-party in order for this party to better target its users.[38] First, the user supplies information to an application that also tracks their location, i.e. a vehicle now has this capability, then that application uses a third-party to sift through the user data, then this data is usually supplied to merchants to match with the appropriate consumer.[39] The user is most likely unaware of this exchange and has not seen the information supplied.[40] To mimic an application on one's phone, the car makes a record of its many interactions with the consumer, some of which contain intimate personal information known to a user, but some do not. In the course of ordinary activities like entering a destination into the car's GPS system, users also unknowingly emit lots of "digital exhaust," or trace data, that leave behind fragmentary bits of information, such as geographical coordinates of a cell phone transmission or an IP address in a server log.[41] How this information is stored may present an avenue for a security breach depending on how a company manages its data storage.

Before explaining how a vehicle stores its user's information, it is helpful to understand, on a technical level, how it obtains this information. A vehicle obtains user

---

[37] Ellen P. Goodman *Self-Driving Cars: Overlooking Data Privacy is a Car Crash Waiting to Happen*, THE GUARDIAN (June 8, 2016), https://www.theguardian.com/technology/2016/jun/08/self-driving-car-legislation-drones-data-security; Andy Sharman, *BMW Sounds Alarm Over Tech Companies Seeking Connected Car Data*, FINANCIAL TIMES (Jan. 14, 2015), https://www.ft.com/content/685fe610-9ba6-11e4-950f-00144feabdc0#axzzE=3PMmNVHKX.

[38] *See e.g.*, *Services* DATASIFT http://datasift.com/ (sifts through consumer data for companies like Facebook and Twitter to better target advertising).

[39] *Id.*

[40] Prepared Statement of the FTC May 9, 2012, *supra* note 16. *See also* Prepared Statement of the FTC, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs,* 109th Cong. (Mar. 10, 2005), available at https://www.ftc.gov/os/testimony/050310idtheft.pdf; *see also* FTC Workshop, *The Information Marketplace: Merging & Exchanging Consumer Data* (Mar. 13, 2001), available at https://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data; FTC Workshop, *Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information* (June 18, 2003), available at https://www.ftc.gov/news-events/events-calendar/2003/06/information-flows-costs-benefits-related-collection-use-consumer.

[41] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, *supra* note 27 at 34.

information through its method of 'communicating'. There are generally two types of communications that car manufacturers install.[42] The first is one that is embedded, and the second more recent type of communication is smart-phone based.[43]

The embedded communication is a subscription that a passenger can opt out of at any time as a one-to-one connection that is secure.[44] For example, General Motors calls its system the "Onstar" system, Toyota calls it a data communication module.[45] The smart-phone based communication system poses a greater security risk. It contains applications that one would have on their phone that use Bluetooth or a USB cord to connect the phone with the vehicle.[46]

There are safety concerns inherent within the vehicle industry's management of a consumer's information. The Federal Bureau of Investigation has issued an official public service announcement about the vulnerabilities that exist within a vehicle's wireless communication functions.[47] These wireless communication functions include mobile devices connecting to a car via USB, Bluetooth or Wi-Fi with a third-party device connected through a vehicle's diagnostic port.[48] It is possible for an attacker to remotely exploit vulnerabilities like gaining access to the vehicle's controller network or to the user's data stored on the vehicle.[49]

The risk that comes with connecting a smart device to the vehicle is that it can be unknowingly be replicated by a hacker who can create a connection by bridging various networks without coming into physical contact with anything.[50] A hacker can access things like the vehicle's brakes or lights, all by accessing the vehicle's internal computing system, sometimes by access to a smartphone.[51] Some vehicles already have a built-in cell phone so a hacker would not need to access a person's cell phone, but can directly access the car through its phone and find information supplied to the GPS, or access the car's immediate

---

[42] Stephanie Gilley, *Federal Trade Commission Internet of Things Workshop*, FED. TRADE COMM'N at 240 (Nov. 19, 2013), https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] Federal Bureau of Investigation, *Motor Vehicles Increasingly Vulnerable to Remote Exploits*, PUBLIC SERVICE ANNOUNCEMENT (Mar. 17, 2016), available at https://www.ic3.gov/media/2016/160317.aspx.

[48] *Id.*

[49] *Id.*

[50] Stephanie Gilley, *supra* note 42, at 243-244.

[51] *Id.* at 244-245.

location.[52] A hacker could also access the headphones in the car used for hands-free Bluetooth capability and listen to passengers' conversations.[53] It is worth noting that only a few years ago courts found an unlawful search where police had to physically trespass in order to track a car's GPS.[54] This exact scenario is already outdated, since GPS can be accessed remotely.

Vehicles have their own computing systems complete with GPS, but so do most other products that connect to the vehicle. Most social media applications have GPS capability that increases the product's functionality. Some applications rely on GPS for their entire business model, like applications that map traffic.[55] Uber, the ride-sharing application, has recently announced it will track a user's location without consent.[56] This means that the application will run constantly and keep track of a person's location, then store and manage this data to improve its location accuracy.[57] As a reminder, the information Uber stores and manages is not regulated, but may be subject to internal standards.

A fair amount of applications usually ask a consumer for permission before accessing their phone's GPS capabilities.[58] However, there is location data attached to every message a person sends from their phone, and technologically advanced criminals have the capability to exploit this.[59] Companies can also access a consumer's location using cell tower signal-based technologies, Wi-Fi Internet access point technology, or crowd - sourced positioning.[60] Assisted GPS, a hybrid technology, uses more than one data collection methodology to access location data, and it is also widely used by most companies.[61]

---

[52] *Id.* at 246.

[53] *Id.*

[54] *See* United States v. Jones, 132 S. Ct. 945 (2012).

[55] *See e.g., Waze Privacy Policy*, WAZE, https://www.waze.com/legal/privacy (collects user data to map traffic).

[56] EPIC Complaint, *In the Matter of Uber Technologies, Inc., Fed. Trade Comm'n* (June 22, 2015), available at https://epic.org/privacy/internet/ftc/uber/Complaint.pdf.

[57] *Id.*

[58] *See, e.g.*, Kenneth Olmstead and Michelle Atkinson *Apps Permissions in the Google Play Store*, PEW RESEARCH CENTER (Nov. 10, 2015), http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/ (235 different types of permission requests in the Google Play Store).

[59] Hannah Jane Parkinson, *Marauder's Map: the Chrome App that Stalks Facebook Messenger Users*, THE GUARDIAN (May 28, 2015), https://www.theguardian.com/technology/2015/may/28/marauders-map-chrome-app-tracks-facebook-messenger.

[60] Governmental Accountability Office, *Consumer Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not be Clear to Consumer*, GAO-14-649T (June 4, 2014) available at https://www.gao.gov/products/GAO-14-649T.

[61] *Id*.

Most consumers are unaware of the specific information garnered from their device. A recent study shows that sixty-five percent of those American consumers were not aware that companies could share their data with other companies.[62] There are also no laws against company employees reading customer-supplied information. This is demonstrated by an application for note taking that recently announced it would increase its capability if consumers allowed its employees to read through consumers' personal notes.[63] Before the application installed its opt-in option, or gave consumers a choice, it unilaterally changed its privacy procedures to allow its employees to be able to read through any consumer-supplied notes. It was not until the application told its consumers about this new feature that it switched to the opt-in ability due to public outrage.[64]

In another instance, the FTC fined a social networking application for $800,000 because it obtained user information without their consent.[65] This settlement required the company to conduct an audit every other year for the next twenty years and develop its own privacy policy.[66] The FTC's complaint used the Children's Online Privacy Protection Act Rule, which prevents the unnecessary collection of information from children under the age of thirteen, to punish the company for not protecting children's private information.[67] This leaves adult victims unprotected by current privacy law, and the FTC did not cite any applicable law to punish the company for not seeking consent from adult consumers.[68]

The automotive industry presents a new front with various

---

[62] Joseph Turow, *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*, ANNENBERG SURVEY (June 2015), available at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf, (writing that Americans think it's futile to protect their information against companies as a tradeoff).

[63] Jon Russell, *Evernote Reverses Privacy Policy that Allows Employees to Read Users' Notes*, TECHCRUNCH (Dec. 16, 2016), https://techcrunch.com/2016/12/16/evernote-u-turn/ (reporting that the technology company Evernote, better described as a platform for sharing and taking notes, announced its change in how it handles user data's privacy).

[64] *See generally* Gilley, *supra* note 42, at 259 (a lawyer speaking about his technology-oriented clients"... they understand that the second they lose consumer trust because of undue concern over security or sharing or privacy issues, that this technology will not realize its potential.").

[65] United States v. Path, Inc., No. C13-0448 (N.D. Cal. Jan. 31, 2013), available at https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincc mpt.pdf.

[66] *Id.*

[67] "COPPA", 16 C.F.R. Part 312 (1999).

[68] *See Path*, No. C13-0448.

routes for potential hackers to amass unlawful information about innocent consumers. Social media applications tend to be a component in most computing devices due to their ability to compile a large amount of personal information. Since social media applications use third parties to sift through the information to then direct it at merchants while the company constantly tracks its users using GPS, the company ends up managing and storing considerable sensitive information. These applications end up connecting to a vehicle through the smartphone where they are downloaded initially, and all of these virtual connections create potential pathways for invasion, posing serious concerns for data security.

The new technical landscape presents many opportunities for data breach. Devices store personal information, and all devices can connect with one another, which puts a large burden on the companies that manufacture these devices to make sure they properly manage the information and make sure it is secure even though it is not mandatory they do this. The marketplace drives companies to maintain proper security measures, but these measures do not necessarily shield companies from legal liability.

III. Current Antiquated Laws Do Not Combat New Technological Concerns

Modern privacy law is not comprehensive. There is no law that governs the collection, use, and sale of personal information by private-sector companies.[69] And, as discussed earlier, there are no laws that impose minimum standards on a company to manage consumer data properly.

There are five federal laws relevant to this article that generally address the privacy of consumer data. First, the Federal Trade Commission Act ("FTCA") authorizes the FTC to enforce the prohibition on unfair or deceptive acts or practices in or affecting commerce.[70] The FTC uses its authority under the FTCA to punish companies that do not adhere to their own policies to protect their consumer's personal information.[71]

The Electronic Communications Privacy Act of 1986 ("ECPA") prohibits providers of electronic communications from voluntarily disclosing customer records to the government, with exceptions.[72]

---

[69] FTC STAFF REPORT *supra* note 15 (citing 5 Remarks of Hall, Transcript of Workshop at 180-181) (supporting baseline privacy legislation); *see also* Remarks of Jacobs, Transcript of Workshop at 360 (emphasizing the importance of enforcement "in the meantime").

[70] 15 U.S.C. §§ 41-58, as amended.

[71] *Id.*

[72] 18 U.S.C. §§ 2510-2522. This part of ECPA was originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520 (1964 ed.) (Supp. IV).

ECPA protects electronic communications while they are in transit.[73] The Stored Communications Act ("SCA") protects stored electronic communications from the government.[74] ECPA has been widely criticized for being outdated. It currently gives protection to electronic data that is more recent than 180 days old, but if it's older than 180 days, as almost all of electronic data is, it has no protection against warrantless search and seizure. ECPA serves as an example of a law that was passed before more recent technology was contemplated, so it should no longer apply in the interest of fairness.

The Communications Act of 1934 ("Communications Act") imposes a duty on telecommunications carriers to obtain express authorization from consumers before they access or disclose call location information, subject to a few exceptions.[75] This act requires telecommunications carriers to secure information and to protect information like where customers are located when they make phone calls.[76]

Finally, the Digital Millennium Copyright Act of 1998 ("DMCA"), has a provision that exempts people from liability who circumvent access-control technology or the proprietary knowledge making it open-source, a concept discussed earlier.[77] This exemption is revised every three years and was just revised a few months ago to allow users to circumvent copyrighted protection systems. This means that users have full ownership of their devices, and the software within their vehicles is no longer proprietary software.[78]

A state's Lemon Law could also provide consumers with a remedy when a breach in a car's security system occurs, so that a car's manufacturer may fix the nonconformity and have it replaced sometimes up to three times or receive a pro rata refund.[79] Each state may have a specific set of exceptions that may apply.

There are no specifically tailored federal laws that apply to the Internet-of-Things and its unique set of different interconnected devices. There are

[73] *Id*.
[74] 18 U.S.C. § 2712.
[75] 48 Stat. 1103-1104 (1934), 47 U.S.C. § 605 (1940 ed.).
[76] *Id.*

[77] Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).
[78] Kyle Wiens, *We Can't Let John Deere Destroy the Very Idea of Ownership*, WIRED (Apr. 21, 2015), https://www.wired.com/2015/04/dmca-ownership-john-deere/.
[79] 73 PA. CONS. STAT. § 1951. *See also* Council of Better Business Bureaus, Inc., *Pennsylvania Lemon Law Summary*, Better Business Bureau (Nov. 19, 2012), http://www.bbb.org/us/Storage/16/Documents/BBBAutoLine/PA-LLaddinfo.pdf.

no federal laws that address or mandate how a company manages its data; however, agencies have issued manuals that guide companies through properly operationalizing privacy and data security practices. This includes proper data retention strategies. The FTC has testified in front of the Senate and maintains its position recommending proper legislation for protecting consumer data and maintaining privacy.[80]

IV. Potential for Privacy Law

Many agencies are responsible for consumer privacy and have created best practice manuals to help industries better manage their data.[81] However, there needs to be firm industry-based legislation that mandates security measures for companies to follow in order to quell the harm that social media and the ever-present GPS inflict on consumer privacy. In the meantime, it is safe to assume that the FTC places a higher burden on industries to protect consumer data with no known limit or what measures to take. Those companies who manufacture and design computing devices have sophisticated knowledge about how the intricacies work within each device. This knowledge is not common-place, so each customer relies on such companies to protect their information from active, but unknown virtual attacks and properly manage their sensitive data to prevent them.

Some stakeholders have developed internal industry codes of conduct for performance measures related to data security, but adherence to these measures are not enforced outside of the company, if they are enforced at all.[82] The automotive industry has a code that has been inspired by the National Highway Traffic Safety Administration ("NHTSA"), which has broad authority to regulate motor vehicles and equipment. [83] The NHTSA has encouraged companies in the auto industry to coordinate with one another through participation in the Auto Information Sharing and Analysis Center ("ISAC"). [84] Participation in the Auto ISAC allows a company to safely and quickly share information with other companies about cyberattacks and methods to help prevent such attacks. NHTSA's idea for the Auto ISAC came from

---

[80] Prepared Statement of the FTC, May 9, 2012, *supra* note 15.

[81] I.e. the FTC, the Federal Communications Commission ("FCC"), the Department of Commerce ("Commerce"), National Telecommunications & Information Association ("NTIA"), and the Department of Justice ("DOJ").

[82] Staff of Sen. Edward J. Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, at 10 (Feb. 2015) (hereinafter "Senator Markey Report").

[83] 39 U.S.C. § 30101.

[84] *Senator Markey Report*, *supra* note 82, at 10.

President Barack Obama's executive order.[85] The Executive Order promoted industry cooperation in order to combat cyber vulnerabilities.[86] Participation within the Auto ISAC is voluntary.[87]

Although some industry codes have progressed with governmental input, overall industry codes are often varied. For example, in the auto industry in order to identify the source of its location-based data, some companies may protect this data with de-identification methods that either have a name attached, a unique identification number, a number that changes, or data that is stripped of all identifiers and then aggregated.[88] Not only are the internal data identification measures among companies varied, but so are the data storage policies. Some companies store data on-board the vehicle or locally, and others transfer the data to a central location, or as off-board storage.[89] The off-board storage that contains sensitive data may be managed by the same company or by a third-party company.[90] A Senate-backed study found that most information companies collect is "only as needed for legitimate business purposes," but most companies have not defined what type of information constitutes a legitimate business purpose.[91] The typical repercussions for an employee who violates a company's internal policies on handling customer data vary from losing their job to receiving some sort of disciplinary action.[92] It is worth emphasizing that obtaining a large amount of sensitive customer data can prove very valuable in the marketplace and may be a more economically viable option than keeping one's job or may be worth suffering a demerit.[93]

Privacy advocacy groups and government agencies tend to use something referred to as "Fair Information Practice Principles" to help inspire an outline for security measures that companies can use to protect sensitive information. These "FIPPs" identify measures directed at the customer that will disclose how the company handles their

---

[85] *See Exec. Order Establishment of the Federal Privacy Council* (Feb. 6, 2016), available at https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council.

[86] *Id.*

[87] *Senator Markey Report*, *supra* note 82, at 10.

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] *Id.* at 11.

[92] Govt. Accountability Office, *supra* note 60, at 7.

[93] Steve Lohr, *Data Could Be the Next Tech Hot Button for Regulators*, THE NEW YORK TIMES (Jan. 8, 2017), https://www.nytimes.com/2017/01/08/technology/data-regulators-google-facebook-monopoly.html?rref=collection%2Fsectioncollection%2Ftechnology&action=click&contentCollection=technology&region=stream&module=stream_unit&version=latest&contentPlacement=72&pgtype=sectionfront.

information, offer the customer an educated choice in the matter or their consent, provide transparency in a company's measures or give customers access, provide accuracy in its protection of data, use better data retention policies and data minimization as preventative measure against hackers, promote data security, and provide accountability to the customer.[94] FIPPs are supported by the government as the basis for developing a general initiative for companies to protect information privacy. A few years ago, the NTIA also provided a resource that could guide internal codes and future legislation that was prepared for the White House.[95] This report discussed the existing need to protect consumer privacy in the technical sphere and how to balance promoting innovation in the global digital economy.[96]

The FTC has also issued many reports that specifically detail how to better manage data within the technical community, including one on how to be able to better manage privacy disclosures through mobile applications aimed at children.[97] As its *pièce de résistance*, the FTC has issued a detailed Final Report to the Senate that compiled suggestions from over four hundred stakeholders in technology.[98] This report suggested that companies should only obtain data that is needed for a defined and specific business purpose, then retain that data as long as needed only for that specific purpose, making sure to properly dispose of it after.[99] The FTC Final Report also suggested that companies could improve their privacy disclosures, and try to work toward standardizing their practices so that consumers, advocacy groups, regulators, and others can compare each company's data practices and make educated choices among different companies based on those practices thus promoting competition among companies to create the best practices aimed at privacy.[100] The report suggested that these required measures would assure consumers that companies respected their privacy. Agency manuals with stakeholder input

---

[94] *See,* Federal Trade Commission, *Privacy Online: A Report to Congress* 48 n.27 (1998), available at https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf; Govt. Accountability Office, *supra* note 60, at 7.

[95] The White House, *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, D.C., Feb. 23, 2012).

[96] *Id.*

[97] Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Washington, D.C. Feb. 2012) available at https://www.ftc.gov/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing.

[98] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington, D.C. Mar. 2012).

[99] *Id.*

[100] *Id.*

could provide helpful resources for companies to follow that could also help them avoid liability to the consumer by adequately protecting consumer privacy in the absence of firm legislation.

V. Current State of Affairs

Social media and GPS go hand in hand, as GPS supplies social media with direct location-based information about a consumer which can better attract advertisers who can target and tailor features of the device to consumer preferences. In reality, the information a consumer willingly provides to social media, coupled with the information an application unknowingly collects, makes up a large portion of their sensitive information stored in an undisclosed location and managed by an unknown security measure to the consumer. Most people have a cell phone that contains a mini-computer on their person at all times, and this cell phone has also become a glorified tracking device that connects to most devices a consumer also owns in this modern age. The modern consumer is largely unaware of how their private information is managed.

Companies that produce computing devices often share a consumer's personal information among its employees, and with other third-party advertisers or data centers, all largely unregulated by the law. The current system gives a criminal easy access to a person's current location, the location of their home, and other sensitive personal information. Sensitive data can come in many forms and the consumer can come in many forms as well, including an employee who shares proprietary information about their company on the device, or shares information about their child. Not only is the owner of such a device fearful that their information is easily shared, but this fear can also spread to many other innocent actors who also have an interest against such private information being accessed unlawfully.

Various agencies have prompted legislative reform, which could diminish the public concern about the security of any private information that comes from social media applications that use GPS. The Internet-of-Things has linked various devices that make a consumer susceptible to harm as a consumer is no longer entirely in control of their private information nor necessarily aware of where that information is stored or whether someone has unlawfully obtained it. In fact, the company who has a duty to manage and secure this information has complete control. Currently, it is up to the company to provide adequate security measures to protect private information, but these measures, if they exist, are often complex and varied. A device can no longer be analyzed by old

industry standards and definitions, since most devices contain a hybrid of functionalities and a myriad amount of information. Social media applications and their corresponding GPS functionalities located on these new hybrid devices present harm to many in the new age because the industries that create such devices are largely unregulated and customers are not kept abreast of who has seen their information, what kind of information can be seen, and how any companies can secure it.