Santa Clara University School of Law

Santa Clara Law Review

Volume 52 | Number 4 Article 3

12-14-2012

Privacy in Autonomous Vehicles

Dorothy J. Glancy
Santa Clara University School of Law, dglancy@scu.edu

PRIVACY IN AUTONOMOUS VEHICLES

Dorothy J. Glancy*

TABLE OF CONTENTS

INTRODUCTION

If people were not involved with autonomous vehicles, privacy would not be an issue. Because people will be

* Professor of Law, Santa Clara University Law School. B.A. Wellesley College, J.D. Harvard Law School. This Article was presented at the January 20, 2012 symposium on "Legal Implications of Autonomous Vehicles." The intrepid autonomous vehicle symposium editors, Tijana Martinovic and Kevin Rogan, deserve great credit both for suggesting this topic and for their remarkable follow-through. Many thanks to Barbara Wendling for helpful guidance about automobile technology and transportation policy. Greatly appreciated research assistance was provided by Nicole Hess.

intended users and purchasers of autonomous vehicles, understanding where and how privacy and autonomous vehicles will interact is important to the success of these new modes of personal mobility. Whenever a person is linked with an autonomous vehicle, privacy interests become important. Among the social and cultural issues that may be "the most slippery territory for autonomous vehicles,"[1] the most challenging are privacy interests.

Privacy norms center on the unique dignity of each individual human person. They are expressed in several types of privacy interests that will affect, and be affected by, autonomous vehicles. For example, autonomous vehicles will affect individual autonomy by taking control over an important aspect of people's lives—the way in which they move from place to place. Autonomous vehicles are also likely to raise concerns about personal information privacy when autonomous vehicles generate personal information about the people who use them. Potential use of autonomous vehicles as tools for comprehensively tracking people's travels affects privacy interests associated with concerns about surveillance. In the future, autonomous vehicles will need to accommodate such privacy interests, just as privacy interests are likely to adapt to autonomous vehicles. This Article explores these synergies.

Two factors complicate thinking about interactions between autonomous vehicles and privacy. First, interactions between autonomous vehicles and privacy are not now a presently observable phenomenon. Not yet marketed as consumer products, autonomous vehicles exist at present only in a variety of prototypes and experimental models. Therefore, it is necessary to project privacy issues onto a future world in which autonomous vehicles without active drivers move people and goods across roads and highways. Second, interactions between privacy and autonomous vehicles involve relationships between two flexible concepts that can be difficult to pin down. Precise details of what consumer versions of autonomous vehicles will be like are not

1. Tom Vanderbilt, *Let the Robot Drive: The Autonomous Car of the Future Is Here*, WIRED MAGAZINE, Feb. 23, 2012, *available at* http://www.wired.com/magazine/2012/01/ff_autonomouscars.

now known.[2] Experimental versions discussed in this Article suggest a broad range of possible configurations. Just about the only characteristic that all autonomous vehicles appear to share is the dispensability of an active human driver. Moreover, privacy is a notoriously contentious concept with a number of different and evolving meanings. As a result, exploring potential interactions between privacy and self-driving vehicles (neither of which has a fixed meaning) is intellectually challenging.

This exploration of privacy in autonomous vehicles begins by contrasting two potential types of autonomous vehicles that, if developed into consumer products, would interact with privacy in different ways. It will then look at some of the different types of potential autonomous vehicle users. Next, the Article examines three types of privacy interests likely to be affected by autonomous vehicles: autonomy privacy interests, personal information privacy interests, and surveillance privacy interests. After considering the reasonableness of expectations of privacy in the context of autonomous vehicles, this discussion will turn to some suggested strategies for optimizing potential synergies between privacy and autonomous vehicles.

I. TYPES OF AUTONOMOUS VEHICLES

Interactions between privacy and autonomous vehicles will depend on the design and operation of autonomous vehicles. A wide range of possible types of autonomous vehicles will apply different technologies to operate motor vehicles in different ways.[3] All of them replace human drivers with artificial intelligence, but do so in different ways.

Because privacy is concerned with individual people, this discussion focuses on personal vehicles that, if not autonomous, would require human drivers to make personal

2. Autonomous vehicles are more than just self-moving, or self-propelled, vehicles. Self-propelled movement is what the word "automobile" connotes. Rather, an autonomous vehicle is operated and controlled by systems of artificial intelligence either inside or outside the vehicle or a combination of internal and external control. Autonomous vehicles, which may also be called "driverless" or "self-driving" vehicles, can take many physical forms and may be powered by any type of engine—electric, internal combustion, hydrogen, etc.

3. *See* Sven A. Beiker, *Legal Aspects of Autonomous Driving*, 52 SANTA CLARA L. REV. 1145, 1146–49 (2012).

journeys on public roads.[4] The potential universe of autonomous vehicles would include trucks, buses, taxis, emergency vehicles, and the like.[5] However, personal autonomous vehicles used by people who have privacy interests are the most interesting in considering privacy issues.

From a privacy perspective, it can matter a great deal how a vehicle's artificial intelligence interacts with the vehicle user and the roadway environment, as well as what data the vehicle sends or receives. When artificial intelligence replaces the driver in a driverless car, the vehicle's autonomous systems will rely on a number of data sources to assess the driving environment and to control the operation of the vehicle. In thinking about privacy, there are considerable differences between two general types of autonomous vehicles. This discussion refers to them as, on the one hand, selfcontained autonomous vehicles and, on the other hand, interdependent autonomous vehicles. These are simply models of groups of characteristics that future autonomous vehicles may have. They are not technical categories, but rather theoretical examples that help in thinking about the interactions between privacy and autonomous vehicles. It is likely that future autonomous vehicles will combine features of both of these models.

Three technological factors distinguish between these two versions of autonomous vehicles and shape the interactions between autonomous vehicles and privacy: (1) where the controlling artificial intelligence is located, (2) how external data, such as information about the roadway around the vehicle, is collected and transmitted to the vehicle and (3) whether internal vehicle data is transmitted beyond the vehicle. As will be explained more fully below, selfcontained autonomous vehicles deal with these factors differently

4. Personal vehicles are typically privately-owned or leased passenger cars, fleet-owned passenger vehicles, or certain types of individually operated commercial vehicles that are ordinarily operated by human drivers on public roadways.

5. Autonomous mass transit vehicles such as public trolleys, light rail, or heavy rail streetcars already exist and pose separate privacy and security challenges for their users. Also not within the ambit of this discussion are vehicles that do not regularly operate on public roadways; such as military transports, mining vehicles, off-road vehicles, or farm tractors.

from interdependent autonomous vehicles.

All types of autonomous vehicles apply artificial intelligence to integrate both internal data from within the vehicle and external data about the environment outside the vehicle. Then the vehicle's analytic processes determine how the vehicle behaves (speed, direction, braking, etc.). Most experimental autonomous vehicles locate most of that artificial intelligence within the vehicle itself. That is why autonomous personal vehicles are sometimes referred to as "self-driving cars." But it is also possible for all or part of the intelligence controlling an interconnected autonomous vehicle to be located outside the vehicle and communicated to the interconnected vehicle over a wireless vehicular network. The selfcontained autonomous vehicle does not connect to such a network and therefore is not subject to external control.

Both the selfcontained and the interdependent autonomous vehicles will rely on internally facing sensors that collect and feed data about how a vehicle and its various parts are operating to a central sensing and diagnostic component that analyzes vehicle data from various parts of the vehicle. Most non-autonomous modern vehicles already contain such sensors. According to a writer in the *IEEE Spectrum*, even in 2009 it took "dozens of microprocessors running 100 million lines of code to get a premium car out of the driveway."[6] Consumers may be aware of these sensors because some of them provide information to an Event Data Recorder associated with air bag systems in most vehicles. Internal sensors can also collect continuous data about vehicle status that is potentially useful to vehicle manufacturers, traffic engineers, insurance companies, and the like. When this vehicle status and operation information is associated with an identifiable individual, the data becomes personal information that is important for privacy purposes. When a vehicle records such internal sensor data, for example through data logging, it is recording personal information about an identifiable vehicle user's location and

6. R. N. Charette, *This Car Runs on Code*, IEEE SPECTRUM (Feb. 2009), *available at* http://spectrum.ieee.org/green-tech/advanced-cars/this-car-runs-on-code/0. By comparison, it takes 6.5 million lines of software code to operate the avionics and onboard support systems of a Boeing 787 Dreamliner. *Id.*

behavior. Some vehicle data may be anonymous. However, absent privacy precautions, much of a vehicle's internal sensor data is potentially linkable to the vehicle user and is therefore personal information that raises privacy issues.

External situational information about what is going on around the vehicle, such as what else is on, or potentially on, the roadway is also necessary for autonomous vehicles to operate. The selfcontained model of autonomous vehicles exclusively uses onboard outward-facing sensors (such as cameras, radar, thermal imaging devices, and LIDAR (light detection and ranging) to collect data about the roadway environment outside the vehicle. Typically, it matches this external information to digital maps within the vehicle. In contrast, the interconnected model of autonomous vehicles is characterized by receiving external roadway situational information through wireless communications networks. The connected vehicle systems currently under development are designed to transmit data about the sending vehicle's internal status (exact location, speed, heading, and the like) as well as about general roadway, traffic, and weather conditions in the vicinity to other nearby autonomous vehicles. Navigational guidance and travel information may also be carried over vehicular networks.

Interconnected autonomous vehicles are characterized by participating in such a vehicular network over which they both send and receive data. Selfcontained autonomous vehicles do not participate in the network at all and therefore retain within the vehicle all of its internal and external data, as well as full control over the operation of the vehicle. Although separated for the purpose of this discussion into two distinct autonomous vehicle models, future autonomous vehicles may well combine features of both models.

A. Selfcontained Autonomous Vehicles Contrasted with Interconnected Autonomous Vehicles

Selfcontained autonomous vehicles are defined by their reliance solely on information generated from onboard the vehicle, which provides data regarding both internal vehicle operations and the external environment. These vehicles typically also have internal maps of the roadways to be traversed. A selfcontained autonomous vehicle will generate, collect, and retain a great deal of information about the

vehicle, its operation, and the status of its user. That information remains entirely inside the selfcontained vehicle unless or until the information is removed. The selfcontained autonomous vehicle is not connected to any vehicular network, is not subject to external control, does not rely on off-board sources of information, and does not communicate vehicle-related data beyond the vehicle itself. This is the general configuration of the experimental Google car.[7]

In contrast, interconnected autonomous vehicles are wirelessly connected to a communications network, or possibly multiple communications networks. Such a vehicle could potentially be controlled through the network, either directly through operational commands sent to the vehicle or indirectly through selective communication of information known to cause the vehicle to behave in a particular way. For interconnected vehicles, the network provides situational information communicated by external sources of information about the immediate roadway environment through which the vehicle is passing. Information transmitted to an interconnected autonomous vehicle may include status messages from other vehicles or persons that share the network, as well as GPS location data, traffic, and weather reports. The interconnected autonomous vehicle also automatically transmits its own internal vehicle status data through the network to nearby vehicles or to other network users.

The United States Department of Transportation (USDOT) is developing this type of vehicular network in its Connected Vehicle Program.[8] Connected vehicles receive over a wireless channel information about the roadway

7. Erico Guizzo, *How Google's Self-Driving Car Works*, IEEE SPECTRUM, http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works (last visited Apr. 22, 2012). The Google Car apparently uses GPS for basic location data, but does not entirely rely on GPS in determining vehicle location.

8. The Interconnected version of autonomous vehicles would use technologies under development in the Connected Vehicle research program. *Connected Vehicle Research*, U.S. DEP'T OF TRANSP.: RESEARCH & INNOVATIVE TECH. ADMIN., http://www.its.dot.gov/connected_vehicle/connected_vehicle.htm (last visited Apr. 22, 2012). The National Highway Traffic Safety Administration is currently studying the application of this Connected Vehicle type of autonomous vehicle. Stephen P. Wood et. al., *The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles*, 52 SANTA CLARA L. REV. 1423, 1426–27, 1429, 1431–34 (2012).

environment, including the presence and behavior of other road users. In the Connected Vehicle Program, this network is cooperative in that a vehicle both receives and shares internal vehicle sensor information (speed, velocity, heading, etc.) with other similarly connected, data-sharing vehicles through what are called vehicle-to-vehicle (V2V) communications.[9] Assuming that it uses the Connected Vehicle systems currently under development, an interconnected autonomous vehicle could also communicate vehicle status data in real time to roadside infrastructure for use by traffic management centers, toll collection agencies, or law enforcement through vehicle-to-infrastructure (V2I) communications or to mobile devices (V2D). Sometimes the array of potential recipients of vehicle data is simply described as vehicle to "whatever" (V2X). For some communications, such as real-time communications with other nearby vehicles, the speed and low latency provided by a technology known as dedicated short-range communications (DSRC) is likely to be essential. For other types of communications, interconnected autonomous vehicles can use various forms of wireless communications, for example, telematics systems such as that used in General Motors' OnStar. If it follows the parameters of the Connected Vehicle Program, an interconnected autonomous vehicle might well use a mix of information and guidance provided to the vehicle over multiple wireless networks.

B. Privacy Comparison

These two contrasting models of autonomous vehicles have very different privacy implications. On the one hand, the selfcontained autonomous vehicle will generate, analyze, and maintain information, including personal information, solely within the vehicle itself. On the other hand, the interconnected autonomous vehicle is designed to interact continuously with an external network. This network either

9. In the USDOT "Connected Vehicle Program," the Core (or Core System), is such an enterprise network for communications among vehicles and between vehicles and other elements participating in the Core, such as traffic management, navigation applications and many other potential users. *Connected Vehicle Core System Baseline Documentation*, U.S. DEP'T OF TRANSP.: RESEARCH & INNOVATIVE TECH. ADMIN., http://www.its.dot.gov/press/2011/connected_vehicle_coresystem_docs.htm (last visited Apr. 22, 2012).

may simply provide necessary information about the external situation for the autonomous vehicle to determine how to operate or may directly control the interconnected vehicle's operation.

Overall, selfcontained autonomous vehicles may seem more private than interconnected autonomous vehicles. That is both because selfcontained vehicle guidance does not receive information or control messages from external sources, and because the selfcontained model does not send internal vehicle status information to or through an external network. The fact that information and control remain inside the selfcontained vehicle also makes this model seem more secure.

Interconnected autonomous vehicles appear more privacy risky because they depend upon vehicular networks that are external to the vehicles. The personal autonomy of users would be affected by an interconnected autonomous vehicle's susceptibility to external control. In fact, an interconnected vehicle could be externally controlled in two ways. First, indirect control could be exerted by manipulating information transmitted to an autonomous vehicle programmed to behave in a predictable way upon receiving such information. For example, the vehicle could be caused to change route by sending it data indicating that the road ahead is blocked. Second, the network could communicate direct operational commands. For example, a network command could stop a vehicle or cause the vehicle to go to destinations not chosen by its user. Were all of the operations of an interconnected vehicle's movements directly controlled by external decision makers, the autonomous vehicle itself would appear to be no longer autonomous. Rather it would be under remote control. Such an externally controlled vehicle would not be driving itself. Instead, it would be driven by a decisionmaker other than the vehicle or its user. It might be called a "puppet vehicle," because the external decisionmaker would control the vehicle as if a puppeteer were pulling the strings of a marionette. In this situation, all personal autonomy of the user would be eliminated.

With regard to personal information privacy, both types of autonomous vehicles are likely to have highly detailed continuous data regarding vehicle location, as well as information about where the user wanted to go, did go, and

what the user could have seen along the way. In selfcontained autonomous vehicles, personal information would be concentrated on-board the vehicle. As a result, the vehicle itself would be a repository of personal information about everywhere its user had traveled, how the vehicle had traveled, and everything encountered along the way. This personal information contained within the vehicle would be vulnerable to hacking, burglary, and potential access by investigators, both private and governmental. Enhanced physical and data security would be essential to protect the privacy of personal information in the selfcontained autonomous vehicle. Moreover, measures such as encryption, personal data minimization, and frequent data destruction would be crucial to protect personal information in selfcontained autonomous vehicles. Real-time surveillance of selfcontained autonomous vehicles would be possible through outside tracking, but not from within the vehicle itself.

An interconnected autonomous vehicle presents more risks to personal information because interconnected vehicles are designed to be engaged in constant network communication of such personal information as the user's real-time location. The vehicular communications network, on which the interconnected autonomous vehicle relies, would have many more potential data breach points at which personal information could be extracted, hacked or might leak out. Any such network would have to provide robust personal information protection and network security measures, including encryption and anonymization, to guard against privacy risks. Indeed, legislation or regulation may require strong network privacy protections for interconnected autonomous vehicle communications networks. The network on which interconnected autonomous vehicles would rely could also be used for surveillance of every interconnected vehicle. That is why privacy protections and strict controls over access to the network will be essential to protect the privacy of interconnected autonomous vehicle users.

Although potential impacts on privacy may seem greater in the context of an interconnected autonomous vehicle, those potential privacy impacts do not mean that one type of autonomous vehicle is necessarily better than another. It simply means that different types and degrees of privacy protection will be needed depending on the types of

technologies represented by the two models of autonomous vehicles discussed here, or whatever combination of technologies is eventually built into future autonomous vehicles.

C. Outliers

One type of autonomous vehicle that has been the object of considerable speculation is not yet available even in prototype. That is an autonomous vehicle with its own imagination, emotions, and capacity for independent judgment. A vehicle with the ability to make spontaneous choices regarding why to travel, when and where to go, and how to get there, completely independently of human initiation or intervention, exists at present only in fiction. If such a vehicle were developed in the future, it might threaten not only the privacy interests discussed here, but also other human values.[10]

Fictional examples of autonomous vehicles with imaginations and emotions, as well as capacities for independent judgment, are usually highly anthropomorphized, with out-sized personalities and uncanny abilities to communicate in human languages or even in Morse code.[11] These fictional autonomous vehicles can be seen in animated films (*Cars*[12]) or romantic fantasies (*Chitty Chitty Bang Bang*[13] and *The Love Bug*[14]) or appear as sidekicks in science-fiction settings such as the *Knight Rider's* smart-talking KITT.[15] Stephen King's menacing Christine in the film of the same name is an extreme example.[16] Popular fiction presents frightening science-fiction versions of autonomous vehicles that are smarter than their users as terrifying vehicular "Hals" capable of thinking independently

10. RAY KURZWEIL, THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY 7–9 (2005). *See infra* discussion of the Singularity at note 31.

11. The menacing trucks in the Stephen King movie, *Maximum Overdrive*, communicated their demands for diesel in Morse code. MAXIMUM OVERDRIVE (De Laurentiis Entertainment Group 1986).

12. CARS (Pixar Animation Studios, Walt Disney Pictures Group 2006).

13. CHITTY CHITTY BANG BANG (Warfield Productions 1968).

14. THE LOVE BUG (Walt Disney Productions 1968).

15. KNIGHT RIDER (Universal Media Studios 2008).

16. CHRISTINE (Columbia Pictures 1983) (The title character is an apparently indistructable 1958 Plymouth Fury consumed by psychotic love for a young man.)

and contradicting human commands.[17] These are not the autonomous vehicles discussed in this Article.

In addition, this discussion does not focus on either robotic or platooned vehicles that are sometimes considered autonomous vehicles. Robotic vehicles have been in use for some time in public transit or paratransit applications. They are programmed by humans to carry out specific repetitive transport between fixed points—for example, transporting passengers or cargo to, from, or through highly controlled environments, such as dedicated lanes or roadways. Among the oldest of these technologies are guide-rail transit systems that have been used for ground transport in and around airports and amusement parks for decades.[18] Such robotic vehicles, pre-programmed by human controllers to operate in fixed ways, are not autonomous vehicles for the purpose of this discussion.

Similarly, platooned vehicles are also not the focus of this privacy discussion. Platoons of wirelessly-connected tightly-spaced vehicles following a lead vehicle[19] do not need a driver in every vehicle because they are controlled by the vehicle leading the group. Aside from a possible lead vehicle driver, who makes all of the decisions for the unit, no active driver control of individual vehicles is needed as the group of

17. Hal was the psychopathic computer in Arthur C. Clarke's science fiction novel *2001: A Space Odyssey* that overruled the surviving astronaut, Dave. "I'm sorry, Dave. I'm afraid I can't do that . . . ." ARTHUR C. CLARKE, 2001: A SPACE ODYSSEY (1968). Such threats are among the possibilities contemplated by those concerned about the singularity, when artificial intelligence becomes smarter than human intelligence.

18. The Denver Airport provides interesting examples of applications of robotic systems. On the one hand, the automated passenger tram has been a big success. *Denver Airport Tram*, VISITING D.C., http://www.visitingdc.com/airports/denver-airport-tram.asp (last visited Apr. 22, 2012). On the other hand, the automated baggage system remains an infamous example of a robotic system that simply did not work. Kirk Johnson, *Denver Airport Saw the Future. It Didn't Work*, N.Y. TIMES, Aug. 27, 2005, *available at* http://www.nytimes.com/2005/08/27/national/27denver.html?_r=1&pagewanted=all.

19. Trevor Mogg, *Ford Boss: The Self-Driving Car Is Essential—and Coming Soon*, DIGITAL TRENDS (Feb. 28, 2012), http://www.digitaltrends.com/cars/ford-boss-the-self-driving-car-is-essential-and-coming-soon/. "Between 2017 and 2025, Ford believes cars will have the technology to reduce the role of the driver markedly, and that many automobiles will be at least semi-autonomous" through "'vehicle platooning' whereby vehicles proceed pretty much bumper to bumper through the use of car-mounted sensors. This will improve safety and save space on roads which will by that time be busier than ever." *Id.*

vehicles moves as a unit or platoon. Both before a vehicle joins a platoon, as well as after the vehicle has disconnected from the platoon, each vehicle is not autonomous and requires a human driver. So long as joining and leaving a platoon is entirely voluntary and personal information is not collected or mishandled as a result of platooning, there are likely to be relatively few privacy issues posed by an unidentified vehicle voluntarily and temporarily following other presumably unknown vehicles.

Moreover, vehicles with automated and assistive features are not the focus of this discussion of privacy and autonomous vehicles. Already available on conventional motor vehicles, such features are attractive to consumers because they enhance safety, comfort, and convenience. At the same time, these features remain under the driver's ultimate control. Rather than being autonomous, in the full sense of self-driving, vehicles with automated or assistive systems remain subject to driver decisionmaking and control. The features are driver assisting, rather than driver eliminating. Even the most sophisticated of the currently available assistive systems—such as self-parking, automatic lane alignment, and adaptive cruise control with automated braking and acceleration—provide driver override and can usually be turned on or off by the driver. Motor vehicles can also be equipped with automated driver warnings and other automated safety functions.

Many of these automated vehicle technologies are aspects of Intelligent Transportation Systems (ITS) now widely adopted throughout the United States and elsewhere in the world.[20] Some of these technologies automate a specific function in ways that cannot be performed by a driver. For example, anti-lock brakes pulse a vehicle's brakes more rapidly than would be possible for any human driver. Some of these automated features are required. For example, in addition to anti-lock breaking systems (ABS), Electronic Stability Control (ESC) is required for all vehicles built after

20. Dorothy J. Glancy, *Privacy and Intelligent Transportation*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 151 (1995) discusses many of these ITS automotive technologies that have been on the road for a long time. For more recent description of ITS technologies, see generally, *Intelligent Transportation Systems*, U.S. DEP'T OF TRANSP.: RESEARCH & INNOVATIVE TECH. ADMIN., http://www.its.dot.gov/ (last visited Apr. 22, 2012).

September 1, 2011 and driven on United States highways.[21] These limited automated features do not make the vehicle autonomous since they do not replace overall control by a human driver.

The psychological importance of driver control in our culture is typified by James Bond's famous cars, specially engineered by "Q" for Bond's missions. James Bond's cars are automated, but not autonomous, vehicles. Typically, Bond vehicles are equipped with elegant and powerful automated and assistive systems. But James himself is always depicted as in charge of the vehicle, not vice-versa, even when he is not literally occupying the driver's seat. Being a super-spy or superhero seems to require always being in charge of one's vehicle.[22] Passively being driven around by an autonomous vehicle just does not fit the active mastery and in-control-at-all-times superhero image. The distinction between a driver who is actively in control of a vehicle, although supported by automated and assistive systems, as opposed to a passive passenger controlled by an autonomous vehicle, can be significant not only for fictional superheroes, but also for privacy as well.

II. AUTONOMOUS VEHICLE USERS

Although autonomous vehicles will not be for everyone, the broad range of potential types of autonomous vehicles is matched by an equally varied spectrum of potential autonomous vehicle users. Since the role of a person using an autonomous vehicle is typically passive, driving enthusiasts, who enjoy driving automobiles for pleasure or for the thrill of controlling a powerful machine, may not want to use autonomous vehicles. In contrast, part of the attraction of autonomous vehicles is the opportunity for an individual, who would otherwise need to be fully engaged in driving, to do something else or nothing at all.

21. 49 C.F.R. § 571 (2011) (Standard No. 126: Electronic stability control systems.)

22. Batman's "Batmobile" is another example. *See, e.g.*, THE 1966 TV BATMOBILE, http://www.1966batmobile.com (last visited Apr. 22, 2012); THE HISTORY OF THE BATMOBILE, http://www.batmobilehistory.com (last visited Apr. 22, 2012).

At least initially, most autonomous vehicle users will be licensed drivers. State legislation allowing autonomous vehicles on public roads now typically requires a licensed driver who is capable of taking control of an autonomous vehicle in an emergency. For example, Nevada, the first state to license an autonomous vehicle for experimental road use requires that there be at least two humans in the vehicle and that one of them must be licensed and capable of driving the vehicle if necessary.[23] Moreover, in the short run at least, autonomous vehicles will have to share roads and highways with human-driven vehicles unless and until there are dedicated roadways for autonomous vehicles.[24]

Some autonomous vehicle users will likely find a sense of security in being kept track of when they travel. Such a "someone is watching over me" message is already a theme in advertising for such telematics services as General Motors OnStar.[25] For some people, being watched over might feel comforting.[26] However, others would find the same watching to be oppressive monitoring by an overbearing agent of social control.[27] For example, those who object to red light cameras reflect this latter attitude of being repelled by indiscriminate monitoring.[28] Of course, to the extent that being monitored is

23. NEV. DEP'T OF MOTOR VEHICLES, LCB File No. R084-11, *Adopted Regulation of the Department Of Motor Vehicles* (2012), *available at* http://www.leg.state.nv.us/register/RegsReviewed/$R084-11_ADOPTED.pdf. NEV. DMV REGULATIONS, LCB File No. R084-11, section 10 (Mar. 1, 2012) [hereinafter NEV. DMV], *available at* http://www.leg.state.nv.us/register/RegsReviewed/$R084-11_ADOPTED.pdf.

24. The near future when there will be a mixture of autonomous and driver-controlled vehicles, will present substantial challenges in terms of integrating autonomous vehicle technology into the existing infrastructure.

25. Other examples of similar driver assistance telematics include BMW Assist, Ford RESCU, Kia UVO, Lexus Link, Lexus Enform, AcuraLink, Honda InterNavi, Mercedes-Benz TeleAid, Nissan CarWings, Toyota Entune, and Volvo OnCall. *Embedded Telematics in the Automotive Industry*, IHS ISUPPLI 10–12 (Nov. 22, 2011), http://gallery.mailchimp.com/e68b454409061ef6bb1540e01/files/Embedded_Telematics_in_the_Automotive_Industry_sw_iS.pdf [hereinafter *Embedded Telematics*].

26. That is one of the major selling points of communications systems such as OnStar. *See, e.g.*, *OnStar*, FACEBOOK, http://www.facebook.com/onstar.com (last visited Apr. 22, 2012).

27. The paradigm of such an agent of social control is Big Brother in George Orwell's novel, *1984*. *See generally* GEORGE ORWELL, 1984 (1949).

28. Nathan Koppel, *On Red-Light Cameras and the Constitution*, WALL ST. J. L. BLOG (Aug. 25, 2011, 5:35 AM), http://blogs.wsj.com/law/2011/08/25/on-red-light-cameras-and-the-constitution/.

a matter of informed choice by the person being watched, choosing to be monitored could be an exercise of personal autonomy.

For some people, autonomous vehicles could enable more autonomy than they now have. For example, disabled persons, the elderly, and those with impaired driving abilities may find that an autonomous vehicle is just what they want and need. For these potential users, an autonomous vehicle would provide enhanced personal autonomy and self-determination about when, how, and with whom to travel. Autonomous vehicles could provide more individual travel choices than they now enjoy, including the otherwise unavailable independence of traveling alone.[29] Nevertheless, for such users there may be a trade-off with privacy. Being linked with an autonomous vehicle is likely to generate a great deal of personal information about where the user is and what he or she is doing, as well as a comprehensive log of places the user visited. For some potential autonomous vehicle users, relying on an autonomous vehicle could pose a Hobson's choice—either to take this autonomous vehicle mode of personal transport that tracks your every movement, or to have no individual vehicle mobility at all.

For persons ineligible to drive, including the elderly, disabled persons, and perhaps children, there is also the risk that future regimes of autonomous vehicles might exercise even greater control over individual choices regarding whether to travel, where to travel, and when to travel. For example, an interconnected autonomous vehicle subject to external control by network commands would be able to prioritize roadway use so that disabled persons, or elderly persons, or other categories of users might also be required to travel before or after rush hours. In short, disabled or elderly persons who care a great deal about their privacy may face what seems to be a devil's bargain: In order to reclaim the ability to travel independently through use of an autonomous vehicle, a person must compromise privacy by disclosing personal information and subjecting herself to external

29. As noted earlier, state law autonomous vehicle licensing requirements, such as those in Nevada (requiring a driverless car to contain at least two people, one of whom is licensed to take over driving from the vehicle), could make this hope illusory. *See* NEV. DMV, *supra* note 23, at § 10.

control. As a result, some disabled people have suggested that, given an autonomous vehicle's potentially adverse side effects, they would rather take the bus.

III. PRIVACY INTERESTS

When autonomous vehicles become a common mode of personal transport, three types of privacy interests will influence public acceptance of autonomous vehicles and possibly result in legal restrictions on how autonomous vehicles can be designed and operated. These three types of privacy interests are personal autonomy, personal information, and surveillance. Separate sections address each of these privacy interests in detail below. Moreover, the extent to which autonomous vehicles present a context in which their users reasonably expect privacy is also the subject of an extended discussion in a separate section. The moral force of all of these privacy interests, as well as of the legal privacy rights associated with them, is based on the dignity of people expected to use autonomous vehicles. These privacy interests also articulate important political considerations regarding the impact of autonomous vehicles on civil liberties and individual freedoms. All of these facets of privacy play vital roles in a well-functioning civil society as well as in providing protections for individual liberty. They are features of individualism and human freedom that face off against authoritarian dominance or manipulation by totalitarian states. They are also potentially compatible with autonomous vehicles.

Conventional legal analysis of privacy commonly splits privacy interests into two branches: autonomy privacy interests and information privacy (or data privacy) interests.[30] However, given the nature of autonomous vehicle technologies, it makes sense to discuss separately surveillance privacy interests that combine both autonomy

30. This bifurcation is the approach of the California courts in describing the privacy interests protected under the California Constitution's guarantee of an "inalienable right to privacy." CAL. CONST. art. I, § 1 (2012). In *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35 (1994), the court described information privacy as "interests in precluding the dissemination or misuse of sensitive and confidential information." According to the court, autonomy privacy refers to "interests in making intimate personal decisions or conducting personal activities without observation, intrusion or interference." *Id.*

and personal information interests. In the context of autonomous vehicles, surveillance privacy interests have added political and psychological significance. Each of these three types of privacy interests, explored in detail below, will affect autonomous vehicles in important ways.

A. Personal Autonomy Privacy Interests

Personal autonomy underlies many types of privacy rights. In an era when discussions about privacy often emphasize digital personal information and the Internet, this may seem surprising. With regard to autonomous vehicles, personal autonomy will be important in decisions whether or not to choose an autonomous vehicle in the first place. Personal autonomy is concerned with individual control and self-determination—people's abilities to make independent choices about themselves. Many individuals identify psychologically with the vehicles they drive and view their vehicles as key instruments of personal choice, power, and control. It is uncertain whether this close identification of personal autonomy with a person's vehicle may be different with regard to use of autonomous vehicles. Were autonomous vehicles primarily used in car sharing, paratransit, or similar applications, rather than in an individual's personal ownership or exclusive use of a specific vehicle, the intensity of psychological connection between a personal vehicle and autonomy could diminish. Nevertheless, some association between personal mobility and individual autonomy will undoubtedly remain.

In general, personal autonomy privacy interests focus on an individual's ability to control such matters as who knows where she is now, where will she go next, when she will depart, how she will get there and with whom, as well as who can predict or decide where, when, and how she will travel in the future. The idea of autonomous people using autonomous vehicles is verbally puzzling, in part because autonomy appears twice. One can imagine a struggle over which autonomy will ultimately prevail—the human's or the vehicle's?[31]

31. This discussion of autonomy is concerned with different issues from those posed by the Singularity, a future in which artificial intelligence surpasses human intelligence and overrides human autonomy. The Singularity

Superficially, autonomy relationships between drivers and autonomous vehicles may appear to be relentlessly inverse—a zero-sum relationship in which the greater the autonomy of the vehicle, the less autonomy is available for the driver, or vice-versa. However, such a view mistakenly assumes that autonomy relationships between vehicles and users are necessarily binary. Rather than requiring all or nothing control, as used in this context autonomy refers to independence with regard to choices and decisions. So long as each autonomous decisionmaker independently chooses a decision, it does not matter that numerous other decisionmakers arrive at the same decision. It is also important that autonomy can be delegated to agents. The format of such delegations can range from a formal legal power of attorney to simply asking someone else to pick up unspecified ingredients for dinner at the grocery store.

As used here, the word "autonomy" is based on an ancient Greek concept that combined "auto," meaning "self," with "nomos," meaning "law." They expressed this idea as "autonomia," a word that literally meant "self-law" and signified to the ancient Greeks "giving oneself one's own law."[32] Autonomy was associated with the authenticity of a person as the author of that person's own actions[33] as well as with a concept of free will that is essential for personal

involves "[s]marter-than-human intelligence, faster-than-human intelligence, and self-improving intelligence." The Singularity focuses on "technologies which, if they reached a threshold level of sophistication, would enable the creation of smarter-than-human intelligence." *What Is the Singularity?*, SINGULARITY INST. FOR ARTIFICIAL INTELLIGENCE, http://singinst.org/overview/whatisthesingularity/ (last visited Apr. 22, 2012). In such a scenario autonomous vehicles might pose serious existential risk to human beings. In discussing "How could an Intelligence Explosion be useful?," Luke Muehlhauser discusses how "humanity faces several existential risks in the 21st century, including global nuclear war, bioweapons, superviruses, and more." Muehlhauser does not mention autonomous vehicles. Luke Muehlhauser, SINGULARITY FAQ, SINGULARITY INST. FOR ARTIFICIAL INTELLIGENCE, Sec. 3.2, http://singinst.org/singularityfaq (last visited Apr. 22, 2012). Nevertheless, if future autonomous vehicles are safer, cleaner, and more reliable than any human, the government might prohibit all driver control and therby eliminate by regulation a major aspect of human autonomy.

32. *Autonomia, n.*, OXFORD ENGLISH DICTIONARY (2d ed. 1989) (Oxford Univ. Press).

33. ARISTOTLE, *Book II*, *in* NICOMACHEAN ETHICS, at § 4, *available at* http://classics.mit.edu/Aristotle/nicomachaen.2.ii.html (last visited Apr. 24, 2012).

responsibility. The Stoics and Epicurus are credited with shaping the ancient concept of autonomy into something like the modern sense of self-determination that remains fundamental to personal responsibility.[34] Thomas Aquinas[35] and Emanuel Kant[36] further explored this ancient notion of autonomy in their theories of individual agency and moral responsibility.

Of course, applying autonomy to a non-human vehicle is shamelessly anthropomorphic. That is also true of many modern uses of autonomy, such as autonomous republics and autonomous under-sea (or Mars) rovers, as well as autonomous vehicles. Autonomy privacy interests, including self-determination, choice, and self-control, reflect the older individual-centered concept of autonomy as an attribute of a person's moral self.

As applied to autonomous vehicles, individual autonomy contemplates delegation of some choices to the vehicle while others are retained by the individual user. Autonomous vehicles can be considered agents, tasked with making particular assigned choices or decisions limited to certain matters. For example, the vehicle may control specific functions (such as choice of speed or route) but be required to follow other choices (such as the destination or when to start) made by an individual human user. In many instances, human choices and vehicular choices will turn out to be congruent or overlapping.

A human individual's choice to use an autonomous vehicle is an exercise of individual autonomy. As a result, autonomous vehicle users will almost certainly determine the purpose or goal of a journey. That decision could be followed by a choice to "delegate" to the autonomous vehicle aspects of how the journey is to be accomplished. In such a scenario, the autonomous vehicle would be seen as subordinate to the user as the user's chosen agent and an instrument of the user's decisions. An autonomous vehicle could be given the power to make the more granular or technical decisions. After all,

34. THE ESSENTIAL EPICURUS: LETTERS, PRINCIPAL DOCTRINES, VATICAN SAYINGS, AND FRAGMENTS (Eugene O'Connor, trans., Prometheus Books 1993).

35. THOMAS AQUINAS, BASIC WRITINGS OF ST. THOMAS AQUINAS, (A. C. Pegis, ed., Hackett Publishing Co. 1997).

36. IMMANUEL KANT, THE CRITIQUE OF PRACTICAL REASON (L. W. Beck, trans., Macmillan Publishing Co. 3d ed. 1993).

autonomous vehicles are "vehicles"[37] used in instrumental ways to accomplish transportation tasks chosen and ultimately controlled by humans. In many situations involving autonomous vehicles, decisionmaking will be blended. A human user may delegate operational choices to vehicle technologies, but retain overall transportation "goals" and high-level choices.

In the context of autonomous vehicles, four aspects of autonomy privacy will have special importance: control, choice, intrusion protection, and anonymity. These features of personal autonomy also interrelate in interesting ways with both personal information and surveillance privacy interests that will be discussed below. Historically, legal rights to autonomy have been associated with control over intimate personal choices, such as decisions regarding contraception[38] and abortion.[39] Today, autonomy privacy laws also require respect for less intimate individual choices. When individual choices are compiled into a consumer profile, this profile can be used as an unchosen "stand-in" for, or alter ego of, an individual. Indeed, future transactions may treat this profile as more real than the actual individual.[40] Such profiling interferes with choice and compromises autonomy by interfering with a person's self-definition. Such an autonomy privacy right to self-definition is sometimes also the focus of privacy tort actions, as well as privacy statutes and regulations.[41] Moreover, since one's location partly defines one's identity, the capacity of autonomous vehicles to locate users could pose hazards for autonomy privacy by influencing users' decisions about where to go. Physical and psychological intrusions by censors or snoopers can also interfere with personal autonomy.[42] Being able to drive

37. The word, "vehicle," comes from the Latin *vehiculum*, meaning an instrument designed or used to transport people or cargo. *See Vehicle, n.*, OXFORD ENGLISH DICTIONARY (2d ed. 1989).

38. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965).

39. *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973).

40. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG., Feb. 16, 2012, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

41. *See, e.g.*, Sidis v. F-R Pub. Corp., 113 F.2d 806 (2d Cir. 1940); Melvin v. Reid, 112 Cal. App. 285 (1931).

42. *See* Stanley v. Georgia, 394 U.S. 557 (1969) (involving the seizure of obscene film from a person's home). Justice Marshall insisted that the:

anonymously is a choice that is part of autonomy privacy. Legal protections for this choice to be anonymous include the Driver's Privacy Protection Act. This federal statute prohibits unpermitted disclosure of driver and vehicle licensing records from state departments of motor vehicles to identify a person.[43]

A functional view of autonomy privacy describes it as operating in two ways—positive and negative.[44] The positive side of autonomy privacy involves a person's freedom to take action and affirmatively to do something, such as make choices. In contrast, negative autonomy privacy involves an individual's freedom from external interferences. Autonomous vehicles will affect both types of autonomy privacy.

Positive autonomy refers to an individual's abilities to take autonomous action and to make autonomous choices. The famous Warren and Brandeis article that launched modern legal concepts of a right to privacy described the positive aspect of autonomy in connection with protecting "the conduct of a noble life."[45] Positive autonomy includes an individual's ability to control that individual's own personality as well as the ability to make decisions about interacting with others,[46] to travel or to stay home.[47] Over the

> Right to receive information and ideas, regardless of their social worth, is fundamental to our free society . . . . [T]he right to be free, except in very limited circumstances, from unwanted governmental intrusions into a person's privacy . . . . If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.

Id. at 564–65.

43. *See* Drivers' Privacy Protection Act, 18 U.S.C. §§ 2721–2725 (2012). The statute has a number of exceptions such as for law enforcement uses.

44. Modern concepts of autonomy are reflected in the duality of freedom. *See* ISAIAH BERLIN, TWO CONCEPTS OF LIBERTY (1958); *see also* E. GOFFMAN, BEHAVIOR IN PUBLIC PLACES 3–12 (1963); E. GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959). *See generally* Charles Fried, *Privacy*, 77 YALE L.J. 475, 475–82 (1968).

45. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 207 (1890).

46. *Id.* at 196, 219–20.

47. Justice William O. Douglas described various zones of privacy, in which an outermost privacy zone protects an individual's "freedom to walk, stroll, or loaf." Doe v. Bolton, 410 U.S. 179, 213 (1973) (Douglas, J., concurring).

last century, court decisions protecting positive autonomy privacy often focused on an individual's rights to control one's own life choices and to make highly personal decisions, particularly with regard to intimate matters, such as sex and procreation.[48] However, much more mundane activities than sex and procreation are also facets of positive autonomy privacy. For example, concerns about positive autonomy privacy motivate the Federal Trade Commission's ongoing efforts to deal with online behavioral advertising.[49] This positive side of autonomy privacy also applies to transportation choices, including an individual's right to determine where to go, how to get there, and when to travel.[50] In the future, when a person chooses either to drive or to use an autonomous vehicle, such a choice will be an exercise of positive autonomy.

The negative side of autonomy privacy was famously characterized by Warren and Brandeis as "the right to be let alone."[51] Negative autonomy privacy means that an individual can prevent access to the individual. It empowers the individual to prevent or avoid external influences, interferences, or meddling.[52] The resulting state of non-interference is negative autonomy privacy. This negative side

48. *See, e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003); Roe v. Wade, 410 U.S. 113 (1973).

49. U.S. DEP'T OF COMMERCE: INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010), *available at* http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf; FED. TRADE COMM'N, REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (last visited Apr. 24, 2012). *See also* In the Matter of Google Inc., F.T.C. Docket No. C-4336 (Oct. 13, 2011).

50. The informal anthem for positive transportation autonomy might be the refrain:

> You gotta go where you wanna go,
> Do what you wanna do
> With whoever you wanna do it with.

JOHN PHILIPS, GO WHERE YOU WANNA GO (Lou Adler 1965). This song was made famous by "The Mamas & the Papas" on their album "If You Can Believe Your Eyes and Ears" from 1966. THE MAMAS & THE PAPAS, IF YOU CAN BELIEVE YOUR EYES AND EARS (Lou Adler 1966).

51. Warren & Brandeis, *supra* note 45, at 195.

52. In the original argument for recognizing a right of privacy in the United States the principle of "an inviolate personality" was one of Brandeis's descriptions of negative autonomy. *Id.* at 205; *see also* Dorothy J. Glancy, *The Invention of the Right to* Privacy, 21 ARIZ. L. REV. 1, 21–28 (1979).

of autonomy protects an individual's positive freedom to make independent decisions "without observation, intrusion, or interference."[53] Many privacy laws protect individuals against unwanted interferences with negative autonomy. Examples include statutes that protect people against cyberstalking[54] and spam.[55] Whether autonomous vehicles will be instruments that facilitate intrusion or will be equipped to prevent intrusion will depend on how autonomous vehicles are designed and built.[56] For example, autonomous vehicle users could be treated as captive audiences for location-based targeted advertising as they drive from place to place. On the road, autonomous vehicles could also be designed to screen out such unwanted interferences. Safeguarding individual autonomy against governmental encroachment is a central purpose of the Bill of Rights to the United States Constitution.[57]

Legal protections against interferences with autonomy privacy in the context of autonomous vehicles are likely to focus on several objectives. These objectives include (1) protecting user decisionmaking and control over whether and how an autonomous vehicle is used, (2) requiring respect for a user's choice and consent with regard to both vehicle operation and information autonomous vehicle travel, and (3) preventing intrusions including unwanted sensory inputs, such as advertising thrust on an individual using an autonomous vehicle.

53. Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1, 35 (1994). Psychological distress from powerlessness, lack of control over one's situation is said to be among the most severe deprivations associated with incarceration and institutionalization.

54. *E.g.*, CAL. CIV. CODE § 1708.7 (2011); CAL. PENAL CODE § 646.9 (2011). According to the National Conference of State Legislatures, at least thirty-four states have enacted similar legislation. National Conference of State Legislatures (NCSL), *State Cyberstalking and Cyberharassment Laws*, NCSJ.ORG (Nov. 13, 2012), http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx.

55. The CAN-SPAM ACT, 15 U.S.C. §§ 7701–7713 (2012).

56. In court decisions, negative autonomy privacy rights against intrusion have ranged from rights not to be bombarded by unwanted information, *e.g.* Pub. Utilities Comm'n. v. Pollack, 343 U.S. 451 (1952), to physical intrusions (such as trespass or physical searches) to capturing personal communications and personal information. Tort law provides for damage actions for intrusion, appropriation, public disclosure and for false light. RESTATEMENT (SECOND) OF TORTS §§ 158, 217, 223, 652E (1977).

57. U.S. CONST. amends. I–X (2012)

Many autonomy privacy issues can be avoided by securing individual users' affirmative choice and consent. However, such consent has to be fully informed to be effective. Because of the complicated technological nature of autonomous vehicles, securing informed individual consent to interferences with user autonomy may be difficult. A major challenge for autonomous vehicle developers will be to make sophisticated technical information about the consequences of using these vehicles understandable by potential users.

A particularly useful way to avoid autonomy privacy problems is through anonymity. Since people sometimes want or need to travel without others knowing when and where they are going, anonymity is likely to be an important choice required by people considering use of an autonomous vehicle. For interconnected autonomous vehicles, assuring anonymity will pose a special challenge. For example, anonymous travel in interconnected autonomous vehicles may raise security concerns about being able to trace misbehaving technology, or to find antisocial activity or to prosecute individuals responsible for unlawful network activities. Nevertheless, as the United States Supreme Court recently recognized, the ability to choose anonymous personal mobility is important for a society that seeks to avoid authoritarianism.[58]

B. Personal Information Privacy Interests

Autonomous vehicles are likely to generate a great deal of data. Some of that data will be personal information because it is associated with individual people. As a result, appropriately coping with large amounts of personal information will pose major challenges for autonomous vehicles. Potential autonomous vehicle users are likely to be reluctant to allow their personal information to be collected or used without knowing what will happen to that information and what the consequences are for the users themselves. Personal information privacy interests related to autonomous vehicles would include such matters as where, when, and how a person moves from geographical place to place, what uses are made of such personal data, why it is being collected, how

58. United States v. Jones, 132 S. Ct. 945 (2012).

it will be used, how long it will be kept, and who will and will not have access to it.

The present location of an autonomous vehicle user, that person's past travel patterns and his or her future travel plans are among the personal information likely to be associated with autonomous vehicles. Such information can be used to annoy an individual user through targeted marketing and advertising. It can also be used to harass an individual through following, stopping and questioning her, or even stealing her identity. Stalkers can use this type of personal information to frighten or harm people. Government agencies, including law enforcement and intelligence agencies, will seek to use personal information from autonomous vehicles to find suspicious individuals for further investigation or to prosecute suspects based on autonomous vehicle data. Personal information from autonomous vehicles about a user's past locations will also be used to predict where the individual is most likely to be found in the future.

Moreover, personal information from autonomous vehicles can be correlated with other information. For example, the location where the vehicle is regularly parked overnight (e.g., in a high-income residential neighborhood) could be used to profile the likely user (e.g., as wealthy) and to predict the user's actions (e.g., likely to shop at high-end retail shops). The profile could also be used to manipulate user choices such as where to travel (e.g., through advertisements for expensive resorts) or to eat (e.g., enticements to visit a five-star restaurant in the next town). Personal information from autonomous vehicles can also be used as part of an individual's data profile that is used as a surrogate for the individual person.[59] At a much larger scale,

59. Alexis Madrigal described this issue as "the leading edge of a much bigger discussion about the relationship between our digital and physical selves . . . . [It] may end up determining who you are when viewed by a bank or a romantic partner or a retailer who sells shoes." Alexis Madrigal, *I'm Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web*, THE ATLANTIC (Feb. 29, 2012), *available at* http://www.theatlantic.com/technology/archive/12/02/im-being-followed-how-google-and-104-other-companies-are-tracking-me-on-the-web/253758/. The European Data Directive, now under revision, treats personal information as a sort of alterego of the information's subject, with important dignitary and human-rights-based interests at stake. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of*

collection of comprehensive personal information from all autonomous vehicles could result in concentration of information about and power over large numbers of individuals that would pose troublesome political issues.

The United States Supreme Court has raised constitutional concerns about trapping people by secretly collecting personal information without the knowledge or consent of the people involved.[60] Personal data retained indefinitely beyond the awareness of the person who is the subject of the information is a nightmare scenario.[61] In the legal realm, aversion to collection and use of personal information by unseen data collectors on the Internet has led to calls for restrictions on such collection of personal information.[62] Government officials, at both state and federal levels, have suggested legal measures to restrict this type of collection of personal information on line.[63] On the road, covert collection of personal information from autonomous vehicles can pose similar problems. Indeed, the United States Supreme Court recognized the problem of tracking people on the road when it unanimously held that tracking a suspect by placing an unseen GPS device on the suspect's vehicle is unconstitutional without a warrant.[64] Developers of autonomous vehicles are in the fortunate position of being aware of these personal information issues in advance, so that autonomous vehicles can appropriately minimize personal data collection.

Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, EURLEX (Oct. 24, 1995), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

60. *Jones*, 132 S. Ct. at 955–57 (Sotomayor, J., concurring); *Id.* at 962–63 (Alito, J., concurring).

61. FRANZ KAFKA, THE TRIAL, (Mike Mitchell, trans., Oxford World's Classics 2009).

62. Julie Brill, *Big Data, Big Issues*, FTC.GOV *available at* http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf (last visited Apr. 24, 2012).

63. *Id.*; THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter WHITE HOUSE PRIVACY REPORT] (last visited Apr. 24, 2012); Press Release, Kamala D. Harris, Office of the Attorney Gen. of the State of Cal., Joint Statement of Principles with Amazon.com Inc. (Feb. 22, 2012), *available at* http://www.ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf.

64. *Jones*, 132 S. Ct. at 949.

1. Autonomous Vehicle Personal Information

Autonomous vehicles will produce and use many types of personal information, such as origin-destination data and real-time location information. Since autonomous vehicles remain experimental, there is no comprehensive catalogue of all of the personal information that may be collected by autonomous vehicles. Detailed behavioral data regarding users of autonomous vehicles, as well as real-time and historic data about an identified autonomous vehicle user's movements in physical space are potential examples. Destination decisions of autonomous vehicle users, as well as the time, place, and circumstances of when such travel decisions are made, reflect the personalities, behavior, and personal preferences of the people associated with these decisions. Standards that specify data elements that autonomous vehicles will collect, use, record, or transmit have not yet been adopted.[65] When these standards are adopted, personal information requirements, such as requiring that information about autonomous vehicle users be anonymous, should be part of them.

Travel patterns of autonomous vehicle users will likely be among the most valuable of the personal information associated with any type of autonomous vehicle.[66] Personal information about a user's present and past locations, activities, and frequent destinations are examples. In the selfcontained autonomous vehicle, retrospective information related to the user could be logged within the vehicle itself. In the interconnected version of autonomous vehicles, this type of data would be transmitted more or less continuously to and through the network. As a result, location data would be available to pinpoint and keep track of the vehicle user,

65. The Society of Automotive Engineers (SAE) has appointed a committee to come up with standards for roadway autonomous vehicles. But these standards are not yet available and do not appear to address personal information. *See On-Road Autonomous Vehicle Standards Committee*, SAE STANDARDS DEVELOPMENT, http://www.sae.org/servlets/works/customer.do (last visited Apr. 22, 2012).

66. For example, experimental models of selfcontained autonomous vehicles, that rely on the vehicle's own sensors for roadway data, require that the journey be patterned in advance by human drivers. Such patterning records how the vehicle is driven by a human driver along the route to be autonomously driven later by the vehicle. Connected to a user such a pattern is personal information.

both in real-time and over time.[67] Transmitting this personal information through a network, as is the design of interconnected autonomous vehicles, would make locating an autonomous vehicle user in real time relatively easy for anyone with access to the network.

Once patterns of frequent travel have been recorded (either by the network for the interconnected autonomous vehicle or within the selfcontained autonomous vehicle), that information can be used to reconstruct a person's past travel and to predict the individual's future destinations. Mobile systems that collect, digitize, and transmit information about a person's present and past locations and travel patterns are already criticized as presenting a serious problem for personal information privacy. As a result, they have been targeted by lawsuits and regulatory initiatives.[68] The sharp and negative reaction to physical tracking by mobile devices is indicative of how sensitive personal information associated with autonomous vehicles is likely to be.

All sorts of potential data users will be interested in autonomous vehicle user information. In addition to autonomous vehicle developers and transportation researchers, entities engaged in marketing, advertising, and political persuasion, as well as law enforcement and intelligence agencies, would all find autonomous vehicle user data highly valuable. For example, vehicle miles traveled by a person on particular roadways could be collected automatically by an autonomous vehicle to provide the basis for charging for use of highways as well as to provide information about roadway demand and performance to land use and transportation planning agencies. In addition, if made available to marketing and advertising agencies, such personal data could also be used to advertise local retail opportunities or to manipulate autonomous vehicle users' decisions about where to shop. Political candidates already

67. Concurring opinions in *United States v. Jones*, 132 S. Ct. 945 (2012), addressed this issue at 955–56 (Sotomayor, J.) and at 963 (Alito, J., concurring).

68. Al Franken, *Privacy and Civil Liberties in the Digital Age*, WIRED, Mar. 2, 2012, *available at* http://www.wired.com/epicenter/2012/03/opinion-franken-privacyliberties/; Chris Foresman, *Google Faces $50 Million Lawsuit over Android Location Tracking*, ARS TECHNICA, *available at* http://www.arstechnica.com/tech-policy/news/2011/04/google-faces-50-million-lawsuit-over-android-location-tracking (last visited Apr. 22, 2012).

use personal demographics and travel patterns in, for example, "commuter issues" campaigns.

One strategy for avoiding problems associated with personal information is to rely on anonymous information instead. For autonomous vehicle purposes, that would require separating information about the vehicle itself from information linked to an individual person and not collecting the latter. Anonymous information derived from autonomous vehicles should be sufficient for such uses as transportation planning, traffic management and the like. The challenge will be to maintain the anonymity of this information, which often gains value when linked to an identifiable person. Unfortunately, there is no permanent, solid divide separating anonymous data from personal information. When linked to an individual human person, such as an autonomous vehicle user or owner, the vehicle data easily becomes personal information.[69] Data mining and relational database techniques can provide such linkage and re-identify seemingly anonymous information as referring to a particular identifiable individual. For example, linking together a database of anonymous aggregated information with other databases can identify a particular individual or set of individuals.[70] That is why simply removing identifiers or even aggregating de-identified personal information from a number of individuals is usually not sufficient to maintain anonymity. Instead, summarizing data so that particular data records no longer exist is the best way to assure that anonymity continues and that personal information is not subject to misuse.

If personal information is collected about autonomous vehicle users, those users deserve an opportunity actively to consent or not to consent to such personal data collection. As noted earlier, securing consent from individuals to collection

69. When autonomous vehicles operating without human drivers are rare, the very presence of the autonomous vehicle on the road may be sufficient to link it with a very limited category of autonomous vehicle owners. The vehicle make and model, as well as perhaps the location where it is seen would likely reveal the owner. Such linkage to an individual results in what had been anonymous information about an autonomous vehicle becoming personal information about the autonomous vehicle's user. *See also* NEV. DMV, *infra* note 74, regarding requiring special license plates for autonomous vehicles.

70. Brill, *supra* note 62.

or use of personal information derived from autonomous vehicles poses a challenging problem because the technologies involved in autonomous vehicles are likely to be difficult for most potential users to understand. Nevertheless, whenever personal information is collected, used, stored, or shared, informed consent from the person involved is likely to be required.

2. Personal Information Regulation

Personal information, such as that likely to be associated with autonomous vehicles, is regulated by an increasing number of state and federal statutes and regulations that govern collection and use, as well as prohibit misuse of personal information. There are also industry standards regarding appropriate practices with regard to personal information.

An example of existing state personal information laws that would apply to personal information from autonomous vehicles are statutes requiring notification of missing or lost personal information—privacy breaches. Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted such legislation that requires notification and remedial action if personal information is lost or disclosed through a data breach.[71] Since the specifics of these data breach laws vary from jurisdiction to jurisdiction, autonomous vehicles operating in more than one state could be subject to privacy breach laws of several different states. A number of states, such as Massachusetts, follow their residents' personal information and protect it, wherever the data moves geographically.[72]

A federal statute regulates one type of personal information likely to be associated with autonomous vehicles—driver and vehicle licensing information. The

71. *See Security Breach Legislation 2011*, NAT'L CONF. OF STATE LEGISLATURES (Dec. 21, 2011), http://www.ncsl.org/issues-research/telecom/security-breach-legislation-2011.aspx. Some states also provide additional protection with regard to vehicle and driver licensing information under state statutes and regulations.

72. Massachusetts Consumer Protection Act , MASS. G.L. ch. 93A (2011) and 201 CMR 17.01–17.05 (Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth) (2012).

Drivers' Privacy Protection Act[73] (DPPA) applies nationwide to personal information required and processed by state departments of motor vehicles for licensing purposes. The DPPA imposes statutory damages for improper use or disclosure of personal information provided for the purposes of licensing drivers and vehicles. The statute protects specified categories of personal information, such as name and address, and provides even more protection for highly sensitive personal information, such as race. So far, the only state that registers autonomous vehicles is Nevada, where autonomous vehicles will be required to display distinctive red or green number plates.[74] In addition, Nevada regulations require a special driver's license endorsement for "a person who holds a driver's license in this State and wishes to operate an autonomous vehicle in autonomous mode in this State."[75]

In addition to federal Constitutional Bill of Rights protections against government intrusion discussed below,[76] federal statutes such as the Electronic Communications Privacy Act (ECPA)[77] and the Federal Communications Act[78] will apply to certain aspects of autonomous vehicle communications, particularly in interconnected versions of autonomous vehicles. Moreover, to the extent that federal agencies collect or receive information about identifiable users of autonomous vehicles, the Privacy Act of 1974 would apply.[79]

There seems to be a significant potential for legislation and regulation that specifically focuses on personal information derived from autonomous vehicles. Such legislation is illustrated by experience with what is called Event Data Recorder (EDR) statutes. Beginning almost ten years ago, a number of states began to enact legislation to restrict access to information recorded by EDRs.[80] For

73. Driver's Privacy Protection Act, 18 U.S.C. § 2721 (2012).

74. NEV. DMV, *supra* note 23.

75. *Id.* at § 5.1. The autonomous vehicle driver's license requires a "G" endorsement.

76. U.S. CONST, amends. I–X. *See* discussion *infra* Part IV.

77. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2012).

78. Telecommunications Act of 1996, 47 U.S.C. § 222 (2012).

79. The Privacy Act of 1974, 5 U.S.C. § 552a (2012).

80. By 2010 at least thirteen states had enacted legislation specifying specific privacy protections for EDRs. *2009-12 Privacy Legislation Related to*

example, California Vehicle Code section 9951 applies to any new motor vehicle manufactured on or after July 1, 2004 that is sold or leased in California and is "equipped with one or more recording devices commonly referred to as 'event data recorders (EDR)' or 'sensing and diagnostic modules (SDM).'"[81] Not only must the EDR be disclosed in the owner's manual, access to personal data derived from these devices requires either consent by the vehicle's owner or a court order. The California statute also specifically requires that telematics subscription services disclose their capacity to record or transmit vehicle diagnostic information as part of their subscription services. Although directed at EDRs and SDMs, this statute will directly apply to autonomous vehicles insofar as they use recording devices similar to EDRs or SDMs. This statute also may potentially apply to other types of vehicle data logging, for example by a selfcontained autonomous vehicle.

In part to provide a modicum of national uniformity, the National Highway Traffic Safety Administration (NHTSA) promulgated extensive regulations standardizing EDRs and EDR data as well as requiring special disclosure language regarding EDRs in vehicle owners' manuals.[82] By the time autonomous vehicles are rolled out as consumer products, there may be changes in the regulatory status of the internal vehicle sensor information currently associated with EDRs. For example, the United States Department of Transportation may decide to standardize internal vehicle sensor information and to require that it be transmitted through a Connected Vehicle network. If so, protection of personal information transmitted through such a network would need to be addressed.

3. Personal Information Privacy Risks

Autonomous vehicles can pose a variety of risks to personal information privacy. To the extent that autonomous vehicles rely on anonymous information and do not generate

Event Data Recorders ("Black Boxes") in Vehicles, NAT'L CONF. OF STATE LEGISLATURES (Mar. 14, 2012), http://www.ncsl.org/issues-research/telecom/event-data-recorder-quotblack-boxes-quot-legi.aspx.

81. CAL. VEH. CODE § 9951(a) (2012).

82. 49 C.F.R. §§ 563.1–563.12 (2011).

or use personal information, they will avoid many of these risks. Simply not having personal information—through limiting personal information collection and not retaining personal information that has been collected—helps to minimize these risks.

To the extent that autonomous vehicles do generate personal information, disclosure or transmission of that information to others aggravates privacy risks. In addition to simple loss or improper disclosure of personal data, access to personal information through legal process is easier when such information is held by someone other than the data subject. For example, constitutional protections do not apply to law enforcement and national security officials when they seek access to personal information, not from the person, but from others who have the personal information.[83] Under the "Third Party Doctrine," a readily available subpoena, court order, or administrative order, often without notice to the data subject, can provide relatively easy access to personal data in the hands of someone other than the person who is the subject of the personal information.[84] No warrant or probable cause finding is required. Because this "Third Party Doctrine" circumvents constitutional privacy protection, which would otherwise require a judicial warrant for government access to the same personal information held by the data subject, information privacy risks are magnified. Personal information derived from autonomous vehicles also would be potentially available to civil litigants and private investigators, in such cases as divorce actions and vehicle accident litigation. If personal information is transmitted by autonomous vehicles to other persons and entities, encryption and data security measures as well as confidentiality agreements and requirements will only be partly successful in protecting the privacy of autonomous vehicle personal information.

Different types of autonomous vehicles will pose different types of risks to personal information. The two versions of

83. United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

84. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009); *see also In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), Misc. Nos. 1:11–DM–3, 10–GJ–3793, 1:11–EC–3, 2011 WL5508991 (E.D. Va. Nov. 10, 2011).

autonomous vehicles (selfcontained and interconnected) described earlier[85] will deal with personal information about users in different ways. In general, more personal information will probably be at greater risk in the interconnected type of autonomous vehicle than in the selfcontained version.[86] The fact that interconnected autonomous vehicles rely on wireless communications to exchange information with other vehicles and network users accounts for some of these privacy risks. Since an interconnected vehicle constantly communicates with the network for situational information and guidance, a user's locations and decisions regarding destinations and changes in route would be automatically and continuously available through the network. Moreover, the device identifiers of interconnected autonomous vehicles will likely make all data communicated by interconnected autonomous vehicles at least potentially personal information, unless the device identifiers have been anonomyzed. Even with anonymous device identifiers, any personal information transmitted by the vehicle through a communications network could be vulnerable to unpermitted access unless the data is encrypted and the network is very secure. As a result, in an interconnected autonomous vehicle, personal information would need to be robustly anonomyzed, strongly encrypted, and securely protected to avoid being vulnerable to access, use, and sharing within the network by other network users, the network's controlling entity, or unauthorized interlopers.[87] In the end, privacy risks to users of interconnected autonomous vehicles would largely depend on how the network connecting interconnected autonomous vehicles is designed, managed, and operated.

In contrast, the selfcontained autonomous vehicle does not use wireless communications and is not connected to a network. Instead, the selfcontained autonomous vehicle relies on its own outward-facing sensors for information about driving conditions and roadway situations. Such a vehicle

85. *See supra* Part I.A–B.

86. Of course most autonomous vehicles will combine these types of artificial intelligence. However, considering these types as models will help in seeing some of the differences autonomous vehicle design makes with regard to personal information privacy.

87. Wood, et al., *supra* note 8 at 1462–64.

relies on its own inward-facing sensors for internal vehicle-related data. As a result, the vehicle itself could become a concentrated repository of all sorts of personal information, including a user's travel patterns, highly detailed behavioral information, and perhaps the activities of people outside the vehicle within range of the vehicle's sensors. Although less useful for real-time remote tracking of its user, a selfcontained autonomous vehicle could nevertheless hold retrospective personal information such as highly detailed information about its past locations as well as interactions between the vehicle and its user. The privacy risks would come from unauthorized access to stored, in-vehicle personal information both about the user and about everyone and everything the vehicle has encountered. Strong security measures—from intense physical security to data encryption and access authentication—would be essential for protecting the privacy of personal information generated by selfcontained autonomous vehicles. Using force or falsehoods to gain the user's consent to access personal information contained in the autonomous vehicle would present yet another category of privacy risk.

Appropriate design of autonomous vehicles can of course minimize risks to personal information.[88] Use of anonymous information, rather than personal information, can provide additional protection against risks to personal information privacy interests described here. Assuring that autonomous vehicles only collect, transmit, or use personal information with the knowledge and informed consent of the person using the autonomous vehicle, will also be important to reducing privacy risks in all types of autonomous vehicles.

C. Surveillance Privacy Interests

Surveillance privacy interests respond to people's aversion to being constantly watched, tracked or monitored as they travel from place to place. At the same time, surveillance privacy interests also reflect political and philosophical opposition to pervasive scrutiny of everyone who travels, particularly if that scrutiny is controlled by government. These underlying political implications of

88. *See* discussion *infra* Part V (regarding optimizing privacy and autonomous vehicle interactions).

surveillance are sometimes captured by the age-old question: "Who watches the watchmen?"[89] In fact the challenge of keeping in check those who have concentrated knowledge about how people live their lives and move about in the world seems even more intense in the digital twenty-first century.

Use of autonomous vehicles for surveillance purposes, could compromise something more than just autonomy and personal information privacy interests of individuals. Indeed, surveillance using autonomous vehicles could threaten the political and social well-being of our society. As Supreme Court Justice Sonia Sotomayor noted in her concurring opinion in *United States v. Jones*, "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[90] She also pointed out that "making available at a relatively low cost such a substantial quantum of intimate [GPS location] information about any person whom the Government, in its unfettered discretion, chooses to track," may "'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[91] Surveillance privacy interests reflect these societal concerns about the importance of individual privacy as the foundation of a free society.

Surveillance is a relatively modern idea. Even the word, "surveillance," is fairly new to the English language. It was borrowed from the French by the British at the turn of the nineteenth century to refer to looking over an area, usually from a high place, for strategic information about a battlefield or prospective confrontation.[92] Early in the twentieth century, surveillance usually suggested use of technology to enhance human abilities to see over wide distances to collect comprehensive information about an adversary.[93] Since then,

89. This phrase is translated from Latin: "Quis custodiet ipsos custodes?" JUVENAL, SATIRE VI, (ca. 55 AD) lines 347–48.

90. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

91. *Id.* (citing United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

92. *Surveillance, n.*, OXFORD ENGLISH DICTIONARY (Oxford Univ. Press 2d ed. 1989).

93. For example, aerial reconnaissance became a major factor around World War I. *See* Nicholas M. Short, Sr., *History of Remote Sensing: In the Beginning;*

the word, "surveillance," has been used in a wide variety of careful-watching contexts from medical surveillance of diseases and immune responses, to physical stakeouts of crime suspects, to mass-scale electronic and network surveillance for gathering intelligence or for seeking evidence of anomalous or criminal behavior. Surveillance is also a psychological technique used to affect human behavior through pervasive monitoring of activities and areas to discourage people from violating rules or laws.

Although surveillance most often means covert collection of information, it can also refer to overt watching aimed at modifying the behavior of those watched. An example of overt surveillance is red-light cameras. These devices are often prominently placed as ever-present watchers at intersections so that drivers are deterred from entering intersections while the stoplight is red.[94] One purpose of overt surveillance is to affect the behavior of those being watched, to assure that individual behavior conforms to societal norms. If an autonomous vehicle user were informed that his or her vehicle continuously reports its speed to law enforcement authorities, that user would be more likely to direct the vehicle to conform to the speed limit, rather than exercise personal autonomy in deciding not to conform.[95] Similarly, autonomous vehicles could overtly monitor the behavior of vehicle users so that instances of user activities such as smoking or drinking alcohol are sensed and recorded.

One purpose of overt surveillance is to interfere with individual autonomy through the power of scrutiny. Even potential scrutiny can be sufficient to control behavior, as Jeremy Bentham suggested in his design for the Panopticon Prison.[96] Such direct, announced interference with personal

Launch Vehicles, FAS.ORG, http://www.fas.org/irp/imint/docs/rst/Intro/Part2_7.html (last visited Apr. 22, 2012).

94. Koppel, *supra* note 28.

95. Some insurance companies promote devices that monitor and reward or punish driver behavior (e.g., speeding, sutten starts or stops, driving at dangerous times in dangerous places, etc.) in terms of lower or higher insurance premiums. For example, Progressive Insurance's SnapShot program urges drivers to use a tracking device to keep track of driving habits in order to qualify for a discount. *See Snapshot Common Questions*, PROGRESSIVE INSURANCE, *available at* http://www.progressive.com/auto/snapshot-common-questions.aspx (last visited Apr. 22, 2012).

96. *See* MICHAEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE

autonomy would likely seriously impair trust and confidence in autonomous vehicles. As a result, developers of autonomous vehicles would be unlikely to equip autonomous vehicles for overt surveillance, unless a government regulation required it.

Covert surveillance by autonomous vehicles secretly collecting and reporting personal information seems more likely. Such surveillance is often conducted remotely so that it remains hidden from those being monitored. Given the sophisticated technologies applied in autonomous vehicles, technically unsophisticated users may not understand an autonomous vehicle's potential surveillance capabilities to collect, store, or share personal information about its user. These covert surveillance capabilities include both targeted surveillance of a particular person and mass surveillance of groups or populations.

1. Targeted Surveillance

Targeted surveillance keeps track of a particular identified human person, who would otherwise expect to be let alone, and certainly not to be followed. Such surveillance nearly always involves surreptitiously collecting detailed personal information about the targeted individual and keeping track of the target's every move. Usually, this type of information collection is not conducted openly. For example, assume that an autonomous vehicle generates personal information about a user's location in real time without the user's knowledge or consent. If communicated beyond the vehicle, this real-time information would make it possible to locate the targeted user all of the time, as well as to maintain a comprehensive record of all the places the user has been. When this personal information is transmitted or disclosed to recipients unknown to the target, such surveillance compromises both autonomy and personal information privacy interests. This is the type of vehicle tracking that, because no warrant authorized installation of the tracking device, was held unconstitutional by the United States Supreme Court in *United States v. Jones*.[97]

PRISON (1979).

97. United States v. Jones, 132 S. Ct. 945, 949 (2012).

Unless personal information from autonomous vehicle is encrypted and rendered anonymous, interconnected autonomous vehicles communicating location and other data back and forth over a wireless network could be very useful tools for invisible targeted surveillance. Absent data encryption and anonymity, access to an autonomous vehicle network would enable immediate remote access to the real time location of an autonomous vehicle and its user. Such access would also enable collection of longitudinal records of past locations. As a result, access to the interconnected autonomous vehicle network, would enable law enforcement, national security, and other types of public and private agencies to conduct remote surveillance of the vehicle's user. When a third party, such as a network operator, is a repository of personal information collected through such surveillance, privacy protection would be even further compromised.[98] This personal information held by third parties would be available to government and private sector investigators through subpoenas or administrative orders, without the target of the surveillance ever knowing that the information exists. Indeed, law enforcement access to certain stored personal information from such a network may require neither probable cause nor a warrant.[99]

A selfcontained autonomous vehicle could also be tracked and its user targeted for surveillance in real time. However, the vehicle itself would not be transmitting the surveillance information. Unless connected to a network or attached to a tracking device, a selfcontained autonomous vehicle would not itself enable remote real-time tracking. However, to the extent that the vehicle keeps historical information, such as

98. *See* discussion of Third-Party information *supra* text accompanying note 83 and *infra* Part IV. In her concurring opinion in *United States v. Jones*, Justice Sotomayor suggested that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring); *see, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435, 443 (1976). Justice Sotomayor also noted, "This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

99. Stored Communications Act, 18 U.S.C. 2701–2712 (2012). *See In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114 (E.D. Va. 2011).

past itineraries, about the surveillance target, that information could be extracted from the selfcontained autonomous vehicle by those with access to the computer systems inside the vehicle. Unlawful access by breaking into the vehicle would possibly be deterred by burglary and other laws. Law enforcement extraction of surveillance information from a selfcontained autonomous vehicle would likely require at least probable cause as well as a warrant.[100]

Use of autonomous vehicles comprehensively to keep track of the whereabouts of a targeted individual in all places and at all times can exert substantial control over that individual. Maintaining centralized information about an individual compromises individual self-determination and autonomy and can be harmful to the individual's psychological health. Comprehensive centralized surveillance systems concentrated on an individual can also influence the individual's future choices by keeping track of each time that individual visits socially or politically "unacceptable" locations. The New York Court of Appeals described the impact of targeted surveillance: "Disclosed in [tracking] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[101]

Targeted surveillance compromises an important aspect of individual autonomy—the ability to resist being categorized, manipulated psychologically, intimidated, or mechanistically predicted by society or the government. When an individual is subject to being constantly watched, that person does not feel free to question or to oppose those in charge of the surveillance system.

2. Mass Surveillance

Mass surveillance involves indiscriminate and comprehensive collection of personal information from

100. *See* discussion of Fourth Amendment issues *infra* Part IV.

101. People v. Weaver, 12 N.Y.3d 433, 441–42 (2009). Justice Sotomayor quoted this passage in her concurring opinion in *Jones*, 132 S. Ct. at 946, 955–56.

everyone within an area or sector. This type of large-scale surveillance of a population can also function as an instrument of control over the behavior of every individual within that population. Jeremy Bentham suggested this use of mass surveillance in his design for an efficient prison which he called the panopticon—all-seeing device.[102]

Applied to autonomous vehicles, mass surveillance could seek to collect personal information about all those who use autonomous vehicles. Such mass surveillance would collect and define behavior patterns of autonomous vehicle users. These profiles could later be useful for such purposes as (i) creating algorithmic profiles of typical autonomous vehicle users, (ii) predicting each autonomous vehicle user's individual behavior, or (iii) finding one autonomous vehicle that may or may not be behaving according to prescribed patterns.

Mass surveillance is sometimes confused with intense, comprehensive surveillance of a targeted person. For example, surveillance of the suspected drug dealer, Antoine Jones, in *United States v. Jones* constructed a comprehensive pattern, or mosaic, of highly detailed information about Jones's activities and used that mosaic to locate his drug stash house.[103] Real-time information from the GPS surveillance device attached to his vehicle allowed law enforcement to follow Jones and to see him traveling to the stash house where he was arrested. Just about every investigative tool in the law enforcement surveillance arsenal was used against Jones: wiretaps, physical following, fixed-camera surveillance, as well as attachment of a GPS tracking device to his vehicle, so that the device automatically and continuously located Jones and recorded his every movement. However, the GPS tracking was crucial; and it was the warrantless installation of the GPS device that caused the United States Supreme Court to overturn Jones's criminal conviction. These efforts by law enforcement to follow Jones everywhere and to collect detailed information about what he was doing and with whom he was doing it all of the time was intensive, comprehensive targeted surveillance using massive resources. But such tracking was not mass surveillance,

102. *See* FOUCAULT, *supra* note 96, at 195–228.
103. *See Jones*, 132 S. Ct. at 946.

since the government has not yet tried to watch everyone in the District of Columbia as intensively as law enforcement agencies targeted Jones. Nevertheless, the potential for scaling up the type of massive surveillance used to convict Jones into region-wide mass surveillance of all persons, including those not suspected of criminal activity, troubled some of the Justices who decided *Jones*.

Mass surveillance operates at a different level from the comprehensive surveillance that targeted Jones. Instead, mass surveillance indiscriminately collects personal information about large numbers of people on a population-wide basis.[104] Usually mass surveillance is covert so as not to affect the patterns of human behavior being recorded. But mass surveillance can also be overt, as Jeremy Bentham suggested for the Panopticon Prison.[105] Automated photo-radar is sometimes used in this open way to deter speeding by announcing that all vehicles on a particular road will have their speeds and license plates recorded, and driver photographs taken, so that citations can be sent automatically to those who were speeding. Some towns engage in overt mass surveillance when they post signs that a photograph of every vehicle and its license plate is taken upon entering or leaving the municipality.[106]

Mass surveillance that collects personal information from everyone on the road is not necessary for most transportation management and planning purposes. Anonymous data identifying neither vehicles nor drivers is sufficient for calculating traffic flows or road usage for transportation management and land use planning purposes. For example,

104. Mass surveillance literally gathers up all available information about all persons within range of the surveillance. Officials hope that some of this personal information may turn out to be relevant to investigative or intelligence issues. The hated general warrants in pre-revolutionary America outlawed by the Fourth Amendment were a form of mass surveillance. *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974). Sometimes called "dragnet" surveillance, mass surveillance has been analogized to Forrest Gump's famous aphorism: "Life is like a box of chocolates, you never know what you are going to get." Similarly, "Mass surveillance is like a box of chocolates, police never know what they are going to get." FORREST GUMP (Paramount Pictures 1994).

105. FOUCAULT, *supra* note 97, at 195–228.

106. *See* Will Jason, *Tiburon's Roadside Security Cameras Set to Go Live Soon*, MARIN INDEP. J. (July 27, 2010), *available at* http://www.marinij.com/marinnews/ci_15616255.

cameras recording roadway traffic flows often use low-resolution optics incapable of capturing specific vehicles or license plates. Loop detectors or other sensors that do not identify particular vehicles are used to collect information about how many vehicles use particular road segments at particular times and how fast vehicles in general are moving on those segments. In contrast, more precise roadway surveillance that collects specific identifying information about each vehicle or person on a roadway facilitates use of that information for purposes other than counting cars or determining traffic speeds. For example, roadway surveillance that identifies vehicles or drivers may be used to enforce traffic laws, as well as to find or to follow a particular person for further investigation.

Roadway surveillance information that collects personal data about everyone is often used to compile profiles of people who use particular routes. Mass-collected personal data profiles of individuals' travel patterns can be used not only by law enforcement, but by marketers and advertisers who use the data to predict and manipulate future consumer behavior, for example through direct behavioral advertising. Such detailed personal information about an autonomous vehicle user's locations and on-road behavior can be highly valuable both to the government and to private sector enterprises of many different types, such as news media, private investigators, insurance companies, vehicle product manufacturers, and political campaigns.

The interconnected version of autonomous vehicles could enable mass surveillance in the form of comprehensive, detailed tracking of all autonomous vehicles and their users at all times and places. The networked nature of this type of autonomous vehicle involves a communications network that transmits and receives information related to each particular vehicle. Being able to identify specific devices may be necessary for network security. But, unless measures are taken to assure anonymity as well as data security, the resulting comprehensive personal information collection could be used to profile, predict, and perhaps manipulate the behavior of the vehicles and their users. Law enforcement, private investigators, advertisers, and marketers will all be eager to seek access to an interconnected autonomous vehicle network, as well as to the personal data transmitted through

such a network, unless the network is carefully planned to preserve and protect privacy.

It is interesting to note that selfcontained autonomous vehicles could be used for a different type of mass surveillance. These vehicles rely on arrays of externally facing sensors that will continuously collect detailed information about the roadway environment surrounding the vehicle. Information from these sensors is processed by the vehicle's analytic systems that enable the vehicle to distinguish toddlers from fireplugs. As a result, the selfcontained vehicle will collect detailed data about everywhere the vehicle travels, as well as everything and everyone encountered. In some ways, a selfcontained autonomous vehicle operates as a "mobile panopticon" that moves along roads and highways and literally takes in all details about what is going on in the areas through which the vehicle travels. Based on such mass surveillance concerns, Federal Communications Commission imposed sanctions on Google, for collection of wireless information by "Street View."[107]

Mass surveillance collection and use of personal information about large numbers of people also compromises autonomy privacy interests. Surveillance systems—whether they are law enforcement programs, traffic management systems, or private marketing systems—all directly affect the autonomy of travelers by overriding individual control over who or what watches and keeps track of their movements from place to place. When the government controls such universal surveillance, political concerns about centralizing too much power in a potentially overbearing state reinforce privacy concerns. Authoritarian systems can misuse such mass surveillance systems to round up suspects or to treat individuals or whole categories of people as undesirable or deserving sanctions based on where they are or where they have been. Personal mobility is an aspect of people's lives that totalitarian political systems particularly seek to control.

Travelers forced to look over their shoulders for surveillance systems are affected both by knowing and by not

107. Fed. Commc'ns Comm'n, "In the Matter of Google, Inc." F.C.C. Order No. DA 12-592 (April 13, 2012), *available at* http://transition.fcc.gov/DA-12-592A1.pdf.

knowing whether or when others are watching their actions or capturing personal information about them. Particularly when a person chooses to do something unconventional or considers going to a potentially notorious destination, such uncertainty can be stifling.

IV. EXPECTATIONS OF PRIVACY IN AUTONOMOUS VEHICLES

Whether autonomous vehicles present a context in which people can and should expect protection for privacy interests is a contentious issue. In legal evaluations of privacy claims, "reasonable expectations of privacy" analysis is a familiar way to make an initial determination whether legal protection for privacy interests would be appropriate under particular circumstances. Inquiring into reasonable expectations of privacy in the context of autonomous vehicles asks whether society should protect privacy in this setting, in light of other societal interests, such as safety, convenience, economic, and environmental concerns.

Reasonable expectation of privacy analysis is normally associated with legal decisions about whether to enforce Fourth Amendment protections against unreasonable searches and seizures by excluding evidence from criminal prosecutions.[108] In addition, reasonable expectations of privacy also play a normative role in determining the "protectability" of privacy interests in tort law,[109] as well as statutory[110] and regulatory[111] law. Asking about whether expectations of privacy are reasonable raises policy issues about whether privacy protection is desirable or appropriate in a particular setting, such as autonomous vehicles. Because autonomous vehicles are not yet available for general use, predictions about privacy expectations regarding autonomous vehicles necessarily have to be extrapolated from experience with other types of vehicles, transportation issues, and

108. *E.g.*, United States v. Jones, 132 S. Ct. 945 (2012).

109. *See, e.g.*, Sanders v. Am. Broad. Co., 20 Cal. 4th 907 (1999).

110. *See*, for example, the federal Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 and California's adopted version at section 1708.8 of the California Civil Code. Both concern physical or constructive invasions of privacy.

111. *See, e.g.*, Department of Homeland Security Regulations that Support Anti-Terrorism by Fostering Effective Technologies, 6 C.F.R. §§ 25.1–25.9. (2012).

intelligent systems.

The concept of reasonable expectations of privacy is often associated with a 1967 United States Supreme Court decision, *Katz v. United States*.[112] *Katz* excluded from evidence in a criminal prosecution defendant's conversations recorded by law enforcement from outside a public phone booth located on a public street. In ruling that the Fourth Amendment "protects people, not places," the Supreme Court rejected basing Fourth Amendment warrant requirements solely on location and interference with property rights.[113] Older analysis had routinely withheld Fourth Amendment protections from activities in public places and from intangible intrusions.[114] After the decision in *Katz*, neither the fact that an activity takes place in a public setting, nor the fact that the evidence seized is intangible forecloses Fourth Amendment constitutional protection for privacy interests. Since most of the personal information generated by autonomous vehicles will be intangible digital data collected in public roadway settings, the *Katz* decision is important in understanding the basis for Fourth Amendment protection for expectations of privacy in autonomous vehicles.[115]

112. Katz v. United States, 389 U.S. 347 (1967).

113. *Id*. at 351–52. Although the defendant's conversations took place in a public location, the Court insisted that "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.*

114. *E.g.*, Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

115. In his concurring opinion in *Katz*, Justice Harlan suggested that deciding what should and should not be protected as reasonable expectations of privacy could be based on "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring). Even in situations where each of the two steps suggested by Justice Harlan is not literally followed, reasonable expectations of privacy analysis is used to balance Fourth Amendment privacy interests of an individual with societal interests. Kyllo v. United States, 533 U.S. 27 (2001). Occasionally "reasonable" expectation of privacy analysis has asked whether a privacy expectation is "justifiable," for example, in *United States v. White*, 401 U.S. 745 (1971) and in *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 616 (1989), or "legitimate," for example, in *Couch v. United States*, 409 U.S. 322, 336 (1973) and *Bartnicki v. Vopper*, 532 U.S. 514, 540 (2001), or sometimes all three, for example, in *United States v. Dunn*, 480 U.S. 294, 315 (1987).

Critics of "reasonable expectation of privacy" analysis, such as Justice

Katz and decisions following it do not mean that all intangible communications in all public places will always be automatically protected as private. But these decisions do suggest that communications among interconnected autonomous vehicles or between autonomous vehicles and roadside infrastructure, other mobile devices or the cloud would be eligible for Fourth Amendment protection. No such cases have arisen yet. The focus in *Katz* on the individual as the basis for privacy rights, rather than the place where the individual is located, makes Fourth Amendment protection for people using autonomous vehicles more likely.

Recent court decisions appear to have turned an important corner toward recognizing expanded constitutional protections for privacy in autonomous vehicles. This is quite a change from the past when privacy expectations of people in vehicles on public roadways were often described as ranging from very low to virtually absent.[116] Past reluctance to find expectations of privacy reasonable in vehicular contexts reflected two now-receding factors: (1) a general notion that public roadways are, by their very nature, not places where people should expect privacy and (2) exceptions to Fourth Amendment warrant requirements that seemingly excluded vehicles from constitutional protection. In the twenty-first century, courts are reconsidering both of these factors. In fact, expansion of Fourth Amendment protection for people in vehicles on public roadways is a noticeable trend in court decisions over the past fifteen years. By the time autonomous

Scalia, complain that reasonable expectation of privacy analysis lacks any "plausible foundation in the text of the Fourth Amendment." Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring). In Justice Scalia's view, the use of reasonable expectations of privacy is blatantly subjective and "self-indulgent." *Id.* Justice Scalia slyly suggests that "unsurprisingly, those 'actual (subjective) expectations of privacy' 'that society is prepared to recognize as 'reasonable,' . . . bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable." *Id.* In his view, the answer to what expectations of privacy are reasonable seems to be resolved by judges deciding what seems reasonable to them. In *United States v. Jones*, 132 S. Ct. 945 (2012), Justice Scalia's opinion for the court refuses to apply *Katz* or reasonable expectations of privacy as the basis for the court's decision. Rather, his opinion focuses on trespass to personal property (Jones's vehicle) that enabled collection of evidence against Jones. *Id.* at 951.

116. *See* United States v. Knotts, 460 U.S. 276 (1983). The Supreme Court in *United States v. Jones*, distinguished *Knotts* as limited to "beeper" technology. *Jones*, 132 S. Ct. at 951–52.

vehicles become accepted consumer products, recognition of reasonable expectations of privacy related to persons in vehicles on public roadways may well be unquestioned.

A. Public Roadway Privacy Expectations

Public roadways are frequently used as illustrations of settings where privacy is not reasonably expected. Roads are contrasted with homes where privacy expectations are high.[117] But that does not mean that no expectations of privacy on public roads are ever reasonable, or worthy of legal protection.[118] Societal interests in managing transportation and roadways so that public roads are not used for nefarious purposes have had enduring importance.[119] At the same time, concerns about surveillance privacy interests and excessive government power in this setting also were recognized early in the history of the automobile.[120] They have become increasingly significant.

Early twentieth century automobiles and paved roads resulted in criminal suspects using vehicles on public roadways to violate the law. Law enforcement agents followed. During Prohibition,[121] the United States Supreme Court upheld many types of law enforcement efforts to stop suspected liquor smuggling.[122] *Carroll v. United States*[123] was

117. Kyllo v. United States, 533 U.S. 27 (2001) (involving the use of a thermal imaging device from a public vantage point to monitor the radiation of heat revealing a marijuana growth inside a person's home).

118. Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N. L. REV. 295, 295–99 (2004).

119. For example, the thirteenth century nightwalker statutes in England, Statute of Winchester, 13 Edw. I, Stat. 2, ch.4 (1285), were among the precursors of twentieth-century vagrancy laws, struck down on void-for-vagueness grounds in such cases as *Kolender v. Lawson*, 461 U.S. 352 (1983), and *Papachristou v. City of Jacksonville*, 405 U.S. 156 (1972). Local anti-cruising ordinances, such as that upheld in *Lutz v. City of York*, 899 F.2d 255 (3d Cir. 1990), are more modern manifestations of law enforcement concerns about roadways. *See also* ROGER D. MCGRATH, GUNFIGHTERS, HIGHWAYMEN AND VIGILANTES: VIOLENCE ON THE FRONTIER (1984).

120. *See, e.g.*, Arizona v. Gant, 556 U.S. 332 (2009); Indianapolis v. Edmond, 531 U.S. 32 (2000).

121. U.S. CONST. amend. XVIII (ratified 1919, repealed 1933). Roadway surveillance continued even after bootleggers ceased to pose a problem after Prohibition was repealed in 1933 by U.S. CONST. amend. XXI (ratified 1933).

122. *Olmstead v. United States*, 277 U.S. 438 (1928), which upheld warrantless wiretapping, reflects another of these efforts to prosecute purveyors of illegal alcohol. *Olmstead* was famously overturned in *Katz* and *Berger v. New*

the most prominent of the Prohibition-era automobile search and seizure cases. This United States Supreme Court decision approved warrantless stopping and searching of cars suspected of transporting contraband liquor, but required law enforcement agents to have probable cause to believe that the cars they stopped were carrying contraband alcohol. The Court's opinion in *Carroll* did not require a judicial warrant before law enforcement agents could stop and search vehicles of suspected bootleggers. But Chief Justice Taft's opinion for the Court took pains to recognize that people on public highways do retain privacy rights. The Court's opinion specifically rejected authorizing law enforcement agents "to stop every automobile . . . and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search."[124] Law enforcement searches of everybody on the road would clearly be "intolerable and unreasonable."[125] Mass surveillance of all people on all roadways would not be permissible under the Constitution. Chief Justice Taft expressed particular concern about interference with the rights of people using the public highways "to free passage without interruption or search unless there is known to a competent official authorized to search, probable cause for believing that their vehicles are carrying contraband or illegal merchandise."[126]

Seventy-five years later, the United States Supreme Court decided in *Indianapolis v. Edmond* that stopping every automobile on a roadway for general law enforcement purposes constitutes a seizure for the purposes of the Fourth Amendment that requires a judicial warrant.[127] The case involved law enforcement roadblocks that stopped vehicles that might be carrying illegal drugs. The Court's decision expressed uneasiness with earlier constitutional analysis that had appeared automatically to exclude public roads from eligibility for privacy protection. Holding that a law enforcement drug interdiction program that stopped all cars along a highway was an unlawful intrusion, the Court

York, 388 U.S. 41 (1967).

123. 267 U.S. 132 (1925).

124. *Id.* at 153–54.

125. *Id.*

126. *Id.* at 154.

127. Indianapolis v. Edmond, 531 U.S. 32 (2000).

refused to "sanction [highway] stops justified only by the generalized and ever-present possibility that interrogation and inspection may reveal that any given motorist has committed some crime."[128] The Court's opinion insists on "drawing the line at roadblocks designed primarily to serve the general interest in crime control." According to the Court, part of the purpose of the Fourth Amendment is "to prevent such intrusions from becoming a routine part of American Life."[129] The Supreme Court's decision in *Edmond* signaled an important shift in policy toward protection of constitutional rights on public roadways. In the Court's view, such protection is necessary in order to prevent dangerous trends toward authoritarian political power.

Since the Supreme Court decision in *Edmond*, courts have increasingly recognized and protected privacy rights associated with vehicles on public roads. In *Arizona v. Gant*, a case involving a search incident to an arrest, Justice Stevens warned against "undervalu[ing] the privacy interests at stake. Although we have recognized that a motorist's privacy interest in his vehicle is less substantial than in his home, . . . the former interest [of motorists] is nevertheless important and deserving of constitutional protection."[130] His opinion noted that "authoriz[ing] police officers to search not just the passenger compartment but every purse, briefcase, or other container within that space" is dangerous.[131] The Court rejected "A rule that gives police the power to conduct such a search whenever an individual is caught committing a traffic offense, when there is no basis for believing evidence of the offense might be found in the vehicle." Such a rule is unacceptable because it "creates a serious and recurring threat to the privacy of countless individuals."[132] The Court emphasized that the character of the threat to the privacy of so many people, "implicates the central concern underlying the Fourth Amendment—the concern about giving police officers unbridled discretion to rummage at will among a person's private effects."[133]

128. *Id.* at 44.
129. *Id.* at 42.
130. Arizona v. Gant, 556 U.S. 332, 344 (2009).
131. *Id.* at 345.
132. *Id.*
133. *Id.*

Twenty-first century courts have been increasingly willing to find and protect privacy expectations on public roads because of concerns about the destructive power of surveillance and wariness about excessive societal control that leads to authoritarianism. As a result, it is likely that if law enforcement agencies were to use an autonomous vehicle communications network to control or to stop an interconnected autonomous vehicle on a public road, such a seizure would be subject to constitutional protection requiring at least a reasonable suspicion of criminal activity.[134] *United States v. Jones* suggests that a warrant may be required before such an intrusion. Moreover, in *United States v. Jones* the Court protected Fourth Amendment personal information privacy interests in data about one's movement from place to place.[135] Use of an interconnected autonomous vehicle communications network to provide evidence of traffic violations, such as excessive speed, also appears to call for Constitutional protection.[136] The Court's decision in *United States v. Jones* specifically requires a warrant before law enforcement agents can legally attach a tracking device to a vehicle and then use the device remotely and continuously to follow a suspect's vehicle on public roadways.[137] Of course, if law enforcement sought to break into a selfcontained autonomous vehicle to retrieve evidence of past locations or activities, such action would also require a warrant.

One of the central issues posed in the *Jones* case was whether Jones had reasonable privacy expectations protected by the Fourth Amendment as he drove his wife's car around the Washington, D.C. area for a month with a government-installed GPS tracking device capturing every move the vehicle and its driver made. During oral argument, members of the Court asked a number of questions about a possible analogy between a person driving a vehicle on which law enforcement had secretly installed a GPS tracking device and

134. Illinois v. Lidster, 540 U.S. 419 (2004) (requiring at least a reasonable suspicion of criminal activity for stopping a vehicle).

135. United States v. Jones, 132 S. Ct. 945 (2012).

136. *Id.* at 958 (Alito, J., concurring). The concurring opinions in Jones are particularly emphatic about this point.

137. *Id.* at 949. Justice Scalia's opinion for the Court is particularly concerned about the intrusion on the vehicle owner's autonomy when law enforcement agents installed the GPS device.

a person wearing an overcoat to which law enforcement agents had surreptitiously attached a GPS device.[138] The implication was that just as an overcoat wearer reasonably expects not to be tracked, a vehicle driver also reasonably expects not to be tracked. This analogy raises the intriguing question of whether using an autonomous car could be in some ways like wearing an overcoat—at least with regard to expectations of privacy. If an overcoat wearer reasonably expects that he or she will not be tracked through an unseen device attached to his or her overcoat, it is at least arguable that an autonomous car user should also reasonably expect that he or she would not be tracked through the autonomous vehicle network. The decision in *United States v. Jones* suggests that, unless a warrant is first secured, automated remote tracking of an autonomous vehicle on public roadways would interfere with reasonable expectations of privacy protected under the Fourth Amendment.

B. Vehicle Exceptions to Fourth Amendment Warrant Requirements

A second factor that in the past seemed to indicate lower expectations of privacy regarding motor vehicles is what is called the "automobile" exception to Fourth Amendment prohibitions against warrantless searches. Although the words seem to imply that automobiles are not subject to Fourth Amendment protections at all, the "automobile exception" never meant that vehicles were completely exempt from Fourth Amendment privacy protection. Nor did the exception ever mean that all intrusions on autonomy privacy and interference with personal information privacy through searches of vehicles were constitutionally permissible. The vehicle exception does not apply to seizures of automobiles at all, although in some cases an automobile search is of a vehicle that has already been lawfully seized. Over time, the application of this exception has become increasingly narrow, to the point that it is unlikely to diminish or adversely affect reasonable expectations of privacy in most

138. *See* Transcript of Oral Argument at 5, 18–20, 31, United States v. Jones (2011) (No. 10-1259), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf (questions from Kennedy, Sotomayor & Kagan, JJ.) (last visited Apr. 24, 2012).

autonomous vehicles.

In its current form, the automobile exception only exempts law enforcement from having to secure a judicial warrant before searching a vehicle after the vehicle has been lawfully stopped. All other Constitutional protections apply, except for the requirement of a judicial warrant before the vehicle is searched. Importantly, law enforcement agents searching stopped vehicles have to establish and document probable cause before any warrantless vehicle search. Three reasons have been asserted to justify this narrow exception: (1) the fact that vehicles are inherently mobile, (2) what is sometimes considered to be a reduced (but not absent) expectation of privacy in a vehicle and (3) historical distinctions between searches of automobiles as compared with dwellings.[139] The first reason has by now become the main justification.

Under the Constitution, all vehicle searches must be reasonable, as well as justified by a finding of probable cause based on objective evidence. This probable cause requirement for all vehicle searches is a tough standard. Law enforcement agents have the burden of showing objective facts that amount to probable cause to believe that a lawfully stopped vehicle contains evidence of criminal activity or contraband. Subjective beliefs and suspicions are insufficient. Only if law enforcement agents have first made a fact-based finding of probable cause are they excused from having to secure a judicial warrant to authorize a vehicle search. Such intrusions on autonomy privacy as searching areas of the vehicle where such evidence might be found have to be based on objective facts demonstrating probable cause.[140] Assuming that a future autonomous vehicle was lawfully stopped, under current interpretations of the automobile exception, the vehicle would be subject to warrantless search only if law enforcement agents had sufficient objective facts to determine that there is probable cause that contraband or evidence of a crime will be found in the autonomous vehicle.

A series of twenty-first century United States Supreme Court decisions have rejected earlier standards that would

139. California v. Carney, 471 U.S. 386, 391–93 (1985).

140. Arizona v. Gant, 556 U.S. 332, 345 (2009); United States v. Ross, 456 U.S. 798 (1982); People v. Panah, 35 Cal. 4th 395, 469 (2005).

have permitted vehicle searches based on law enforcement agents' subjective suspicions.[141] Courts now repeatedly state that more lax police practices than objective findings of probable cause are unacceptable in a democratic society. These days, automobile search decisions, reported and unreported, usually rely on *Gant*[142] to require greater protection for privacy before vehicles can be searched. This trend toward making it more difficult for law enforcement agents to search a vehicle without first having secured a judicial warrant, is based in part on concerns about law enforcement overreaching as well as worries about the potential for remote surveillance such as that denounced in the separate concurring opinions in *United States v. Jones*.[143]

Recent court decisions interpreting the Fourth Amendment have paid increasing attention to enhanced expectations of privacy in the contexts of roadways,[144] of vehicles,[145] and of technologically enhanced searches.[146] Since use of autonomous vehicles will involve all of these contextual factors, privacy expectations in autonomous vehicles should be protected under the Fourth Amendment. Indeed, the full range of privacy interests discussed above—from autonomy to personal information to surveillance—are included in the reasonable expectations of privacy of people who in the future will use autonomous vehicles.

V. OPTIMIZING INTERACTIONS BETWEEN PRIVACY AND AUTONOMOUS VEHICLES

As autonomous vehicles begin to be marketed to people in the United States, privacy protection will help to foster trust in these new modes of travel. Without appropriate legal protections for privacy, autonomous vehicles could well meet "market resistance" from potential users who perceive autonomous vehicles as threats to their privacy. Similarly, assuring respect for user privacy is one of the best ways to

141. *Gant* involved a search of a vehicle incident to an arrest of the driver. *Gant*, 556 U.S. at 344.

142. *Id.*

143. United States v. Jones, 132 S. Ct. 945, 954–55 (2012) (Sotomayor, J., concurring); *Id.* at 957–58 (Alito, J., concurring).

144. Arizona v. Gant, 556 U.S. 332, 345 (2009).

145. *Jones*, 132 S. Ct. at 945.

146. Kyllo v. United States, 533 U.S. 27 (2001).

foster trust and confidence in new technologies such as autonomous vehicles.

The most efficient and effective strategy for optimizing interactions between privacy and autonomous vehicles is through building privacy protection into autonomous vehicles from the start. Being proactive about privacy also helps in strengthening user trust. Such a strategy has been popularized as "privacy by design," a concept derived from values-in-design methodologies long advocated by privacy theorists such as Helen Nissenbaum.[147] The Federal Trade Commission (FTC) has proposed privacy by design as a way to integrate privacy into applications of technology, particularly online technologies.[148] One FTC commissioner described privacy by design as "baking in" privacy, as if a technology application were a cake and privacy a key ingredient.[149] A number of United States companies already follow their own versions of privacy by design to integrate privacy considerations into business models, consumer product design, product development cycles, and new technology applications. Companies such as Microsoft, Google, IBM, and Hewlett-Packard apply privacy by design in developing new products.[150] The White House has also endorsed privacy by design.[151] In the transportation sector, privacy by design was suggested as a useful strategy for Intelligent Transportation Systems as early as 2008.[152]

In Canada, Anne Cavoukian, Ontario's Information and Privacy Commissioner, is a major proponent of privacy by design. She insists that, "Privacy assurance must ideally become an organization's default mode of operation" and describes privacy by design as "a holistic view of privacy

147. HELEN F. NISSENBAUM, PRIVACY IN CONTEXT 1–10 (Stanford Univ. Press 2010).

148. *See* FED. TRADE COMM'N, *supra* note 49; *see also* In the Matter of Google Inc., F.T.C. Docket No. C-4336 (Oct. 13, 2011).

149. Julie Brill, FTC Commissioner, Opening Remarks at W3C Meeting (Apr. 11, 2012) at 1, *available at* http://www.ftc.gov/speeches/brill/120411w3c remarks.pdf.

150. Kashmir Hill, *Why 'Privacy By Design' Is the New Corporate Hotness*, FORBES (July 28, 2011, 10:23 AM), http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/.

151. WHITE HOUSE PRIVACY REPORT, *supra* note 63.

152. TRANSPORTATION RESEARCH BOARD, USING VEHICLE INTEGRATION DATA, PART 2: CROSS-CUTTING VII DATA ISSUES, 87th Annual Meeting, Washington, D.C., Session 682 (Jan. 16, 2008).

protection." It

> prescribes that privacy be embedded directly into the design and operation of not only information technologies, but also of business practices, physical design and networked infrastructure. This broad-based perspective on privacy requires that attention be paid to responsible information management throughout all of the interacting, interrelated, and interdependent elements that comprise organizations and their assorted lines of business.[153]

Ms. Cavoukian's privacy-by-design approach rests on seven foundation principles, beginning with the importance of being "Proactive not Reactive; Preventative not Remedial."[154] Other Privacy by Design principles include Privacy as the Default Setting, Privacy Embedded Directly into Design, Full Functionality (Positive-Sum, not Zero-Sum), End-to-End Security (Full Lifecycle Protection), Visibility and Transparency, and Respect for User Privacy (Keep it User-Centric).[155]

---

153. ANN CAVOUKIAN & MARILYN PROSCH, PRIVACY BY REDESIGN: BUILDING A BETTER LEGACY 1 (2011), *available at* http://privacybydesign.ca/content/uploads/2011/05/PbRD.pdf.

154. *Id.* at 1.

155. *Privacy by Design: The 7 Foundational Principles* explains each of these principles:

1. *Proactive Not Reactive; Preventative Not Remedial*
   The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.
2. *Privacy as the Default*
   We can all be certain of one thing – the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, *by default*.
3. *Privacy Embedded into Design*
   Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

As practiced in Canada, the objective of privacy by design is to restore individual control over personal information while providing organizations a competitive advantage over time. In January 2012, the Ontario Privacy Commissioner's Office broadened its privacy-by-design focus to include autonomy interests and surveillance concerns when it hosted a Symposium, "Beware of 'Surveillance by Design:' Standing Up for Freedom and Privacy." In introducing the symposium, Ms. Cavoukian warned that, "Privacy is absolutely fundamental to freedom. Historically, when societies have morphed from a free and democratic society into a totalitarian state, privacy has been the first thread to unravel. Forfeiting privacy in favour of security, not only represents flawed logic, but is unnecessary—it is a false tradeoff."[156]

---

4. *Full Functionality – Positive-Sum, not Zero-Sum*
   Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it *is* possible to have both.
5. *End-to-End Lifecycle Protection*
   Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.
6. *Visibility and Transparency*
   Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.
7. *Respect for User Privacy*
   Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES 1–2 (2009), *available at* http://www.ontla.on.ca/library/repository/mon/23008/295010.pdf.

156. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Introductory Address at Symposium: Beware of "Surveillance by Design:" Standing Up for Freedom and Privacy (Jan. 27, 2012), *available at*

The first step in privacy by design is a privacy impact assessment before launching a product, technology, or application. In the United States, privacy assessments are already fairly common. They were discussed in connection with the enactment of the Privacy Act of 1974 and were eventually mandated for federal agencies by the E-Government Act of 2002 that regulates personal information contained in federal government records systems. The 2002 E-Government Act mandates a prior Privacy Impact Assessment (PIA) to evaluate the privacy impact of any substantially revised or new federal agency Information Technology System.[157] To the extent that the federal government is involved in creating or managing a communications network for autonomous vehicles, or collects data related to users of autonomous vehicles, a PIA is already required to assess in advance the ramifications of the system in terms of personal information privacy. An effective initial privacy strategy for autonomous vehicles[158] would require privacy impact assessments for all autonomous vehicle projects. Moreover, the substance of these privacy assessments should be expanded so that the assessments consider impacts on autonomy privacy and surveillance concerns, as well as personal information privacy.

In early 2012, the White House proposed a Consumer Privacy Bill of Rights, launched with a report, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (White House Privacy Report).[159] This report suggests that "The Consumer Privacy Bill of Rights

http://www.realprivacy.ca/speakers.

157. E-Government Act, Pub. L. 107-347, Title V, § 208 (2002). Title V is the Confidential Information Protection and Statistical Efficiency Act. Section 208 is entitled "Privacy Provisions" and pertains to privacy impact assessments. As in *Privacy by Design*, privacy assessments broadly apply to federal government personal information systems, although there are a number of exceptions.

158. Applying *Privacy by Design* to autonomous vehicles should begin well before the design stage with farsighted assessment of how these vehicles will affect privacy over the long run. The earlier parts of this Article suggest an outline for such high-level assessment. Autonomous vehicles seem to be precisely the type of technologies that would benefit from careful attention to users' expectations. *Privacy by Design* is a particularly effective business practice for enterprises seeking to develop successful consumer products that will rely on the trust of users.

159. WHITE HOUSE PRIVACY REPORT, *supra* note 63.

should be the legal baseline that governs consumer data privacy in the United States."[160] The White House's Consumer Privacy Bill of Rights seems directly to apply to at least some types of autonomous vehicles, particularly interconnected autonomous vehicles that rely on communications networks.

The personal data that is the focus of the White House Privacy Report privacy is "any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device," such as an identifier used to build a usage profile.[161] This definition appears to describe potential autonomous vehicle networks that would be based on the United States Department of Transportation's Connected Vehicle Program.[162] The White House Privacy Report is concerned about "maintaining consumer trust in networked technologies,"[163] and seeks to work with private sector stakeholders to protect privacy rights of consumers, with or without the need for further legislation. The specific rights included in the White House Consumer Privacy Bill of Rights are Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, and Accountability.[164] Attention to these privacy rights endorsed by the United States President can help to optimize synergies between privacy and autonomous vehicles.

In addition to the White House Consumer Privacy Bill of Rights, many similar privacy principles and even bills of privacy rights have been suggested in recent years. Most outline what are familiarly called Fair Information Practices (FIPs), or Fair Information Practices Principles (FIPPs). Such privacy principles have been endorsed by federal agencies such as the Department of Commerce and the Federal Trade Commission.[165] Many privacy principles have

160. *Id.* at 45.

161. *Id.* at 10 (footnote omitted). The omitted footnote notes that the definition of personal data is similar to the definition of "personally identifiable information" used in connection with the Privacy Act of 1974.

162. *See* discussion *supra* Part I.A-B.

163. WHITE HOUSE PRIVACY REPORT, *supra* note 63 at i.

164. *Id.* at 10.

165. *See* U.S. DEP'T OF COMMERCE: INTERNET POLICY TASK FORCE, *supra* note 50; FED. TRADE COMM'N REPORT, *supra* note 49.

been proposed as self-regulatory standards by industry groups. Of the many industry self-regulatory initiatives, one of the more pertinent to autonomous vehicles is the GSMA Association's[166] 2012 "Mobile Privacy Principles," accompanied by extensive "Guidelines for Mobile Application Development."[167] The GSMA describes its core privacy values as "transparency, choice, and control—putting the user first."[168] The GSMA Privacy Guidelines discuss ways to implement a privacy-by-design proactive approach in a mobile environment. They include explanations of fair information practices in a mobile setting, as well as examples and illustrative use cases. Since autonomous vehicles will share many location privacy issues with mobile applications, the GSMA principles and guidelines illustrate a potential privacy strategy. With regard to transportation technologies, a particularly useful privacy policy strategy for autonomous vehicles is the Vehicle Infrastructure Integration (VII) Privacy Policies Framework (VII Privacy Framework).[169] The VII Privacy Framework was unanimously adopted by the VII Coalition, a public-private group brought together by the United States Department of Transportation to evaluate the feasibility of deployment of a nationwide DSRC network for vehicle safety and mobility.[170] Until it was disbanded in 2007,

166. GSMA (Groupe Speciale Mobile Association) refers to the powerful trade association (including around a thousand mobile telecommunications companies) that promotes the GSM mobile telephone system world-wide. *See Membership*, GSMA, http://www.gsma.com/history/ (last visited Apr. 22, 2012).

167. *Privacy Design Guidelines of Mobile Application Development*, GSMA, http://www.gsma.com/documents/privacy-design-guidelines-for-mobile-application-development/20008 (last visited Apr. 22, 2012).

168. *Mobile Privacy Principles*, GSMA, http://www.gsma.com/documents/mobile-privacy-principles/20005/ (last visited Apr. 22, 2012). Additional GSMA Mobile privacy principles include: Openness, Transparency and Notice, followed by Purpose and Use, User Choice and Control, Data Minimization and Retention, Respect User Rights, Security, Education, Children and Adolescents, Accountability and Enforcement. *Id.*

169. INSTITUTIONAL ISSUES SUBCOMM. OF THE NAT'L VII COAL., VEHICLE INFRASTRUCTURE INTEGRATION: PRIVACY POLICIES FRAMEWORK, (Feb. 16, 2007), [hereinafter VII PRIVACY FRAMEWORK] *available at* http://www.its.dot.gov/research_docs/61vii_privacy_framework.htm. The Framework was drafted by the Institutional Issues Subcommittee and unanimously adopted by the Executive Leadership Team of the VII Coalition.

170. VII refers to "Vehicle Infrastructure Integration," a USDOT program designed to implement the FCC's allocation in 1999 of the spectrum band at 5.9 GHz for dedicated short-range communications (DSRC). The application of this communications spectrum to vehicle-based communications for safety and

the VII Coalition was composed of vehicle manufacturers, as well as state, regional, and federal transportation regulators. Its goal was to facilitate development and deployment of a national Dedicated Short Range Communications (DSRC) system for vehicles.[171] The VII Privacy Framework represents a rare transportation-related example of proactive privacy policies created in advance to govern the rollout of a major new transportation technology. The Framework's policies continued to guide privacy protection as the VII system became part of the IntelliDrive[SM] program and later an aspect of the Connected Vehicle Program.[172] To the extent that autonomous vehicles will use a national DSRC network, the VII Privacy Framework appears directly to apply.[173]

The VII Privacy Framework was conceived as a way to help sync the technical design of VII's advanced vehicle communications technologies with individuals' autonomy and personal information privacy interests, as well as with civil liberties concerns about surveillance. The goal was to assure that the technical design and operation of a nationwide DSRC network would respect reasonable privacy expectations. Between 2004 and 2007, a subcommittee of the VII Coalition painstakingly developed consensus regarding two related documents. These documents first articulate privacy principles tailored to the particulars of the VII's vehicle-based DSRC technologies and then set boundaries for legitimate uses of VII. The process involved important input from a

mobility purposes was launched by the United States Department of Transportation in 2004 as the VII Program. *Id.*

171. DSRC is a radio network at 5.9 GHz (5.850-5.925 GHz) spectrum that features extremely low latency (quick on the uptake) allocated by the Federal Communications Commission in 1999 for vehicle-to-vehicle and vehicle-to-infrastructure communications. Because of the quickness (low latency) of this frequency, DSRC is likely to be needed for V2V communications by the interconnected vehicle type of autonomous vehicles. *See* Robert B. Kelly & Mark D. Johnson, *Defining a Stable, Protected and Secure Spectrum Environment for Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1271, 1281–82, 1289–90 (2012).

172. *Connected Vehicle Research*, *supra* note 8.

173. The VII Privacy Policies Framework defines the National VII Program as a broad complex including "all physical, technical and functional aspects of the subsystems and components used to collect, receive, transmit, store, and/or disseminate data and information, as well as the institutional structures and measures implemented in order to govern VII System users and administrators." VII PRIVACY FRAMEWORK, *supra* note 169.

variety of stakeholders, including privacy advocacy organizations in the development of appropriate privacy policies for DSRC technology. This process was precedent setting in fashioning appropriately tailored privacy policies to fit the VII technology as that technology was being developed. Concentrated efforts to devise privacy policies that would work in the complex world of vehicle regulation, vehicle manufacturing, and the often-multifarious concerns of people who are expected to use and to rely on new transportation technology produced the VII Privacy Framework.

The first part of the Framework contains the VII Privacy Principles that are designed to assure that, to the greatest extent possible, individuals who use VII-equipped vehicles will be able to do so privately and anonymously. Such an objective is sometimes described as minimization of personal information. To the extent that personal information might be needed for specific DSRC applications or services, the VII Privacy Principles emphasize the importance of fair information practices. These practices include as notice and consent, as well as the need for careful protection of personal information and for limits on how long personal information would be retained by the network and those with access to it. The nine VII Privacy Principles begin with Respect for Privacy and Personal Information and include Information Purposes, Acquisition, Notice, Fair Information Use, Information Protection and Retention, Openness, Participation and Accountability. The principles emphasize the importance of anonymity secured, in part, through technical methods designed and built into the DSRC System. Based on OECD privacy guidelines,[174] the principles were presented in the familiar context of Fair Information Practices (FIPs) already widely used in both the public and private sectors in the United States. At the same time, each principle was carefully crafted to apply specifically to the VII program's vehicle-based DSRC communications network. A similar effort will also be needed in shaping privacy protection for autonomous vehicles.

174. OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html (last visited Apr. 24, 2012).

The second part of the VII Privacy Framework regarding Privacy Limits is far more innovative and important.[175] This aspect of the VII Privacy Framework sets boundaries on uses of personal information collected by or through a national DSRC network. These Limits establish clear lines beyond which VII's DSRC network is not to be operated or used. The Limits call out particular potential uses of the VII system that, for policy reasons, cannot be allowed.[176] Such defined policy boundaries are a particularly effective way to build consumer trust and confidence. Being clear in advance about what the technology will and will not do with regard to user privacy is an essential trust-building strategy.

The VII Privacy Limits are organized according to functional areas in which the DSRC network would operate: public-sector transportation, public-sector commerce and toll collection, public-sector regulation and commercial vehicle permitting, law enforcement/investigation, public security surveillance, private-sector commerce, and private-sector transportation. This functional organization adapts the Limits to the practical contexts of particular DSRC vehicle technology applications. The Limits emphasize vehicle owners' rights to remain anonymous through the technical design of the DSRC network, as well as through operational controls over the National VII Program. Voluntary individual user consent and choice set important boundaries with regard to use of personal information derived from the DSRC network. For example, the Limits provide that, except for specific public sector regulation and commercial vehicle permitting applications in which personal information is required by law, individuals using DSRC-equipped vehicles should not be required to supply personal information.

The VII Privacy Policies Framework was developed as a foundation. More detailed privacy guidance and further legislative and regulatory measures were expected to carry out the fundamental privacy protections and expectations

175. VII PRIVACY FRAMEWORK, *supra* note 169 (referring to the section entitled, *Vehicle Infrastructure Integration Privacy Limits on Uses of Personal Information*).

176. For example, Limit 4 provides that "the National VII Program shall not be used by law enforcement for: recording real-time video or voice of vehicle occupants, or . . . off-board control of vehicle driving or maneuvering functions." VII PRIVACY FRAMEWORK, *supra* note 169.

outlined in the Framework. In considering privacy protection for autonomous vehicles, a similar deliberative process of consensus building among stakeholders, including privacy advocacy groups would be wise. A privacy policy framework similarly structured in two parts—one containing principles and the other providing limits to technological applications—provides a useful model for creating an autonomous vehicles privacy policies framework.

So far, there are neither technical nor legal standards specifically addressed to autonomous vehicles. In addition to high-level, privacy-by-design measures, privacy standards need to be included among the legal and technical requirements for autonomous vehicles. Technical criteria regarding such matters as anonymization of personal information generated by and gathered from autonomous vehicles, as well as data encryption standards, need to be adopted for all autonomous vehicles before they are launched into the consumer market. The Society of Automotive Engineers (SAE) On-Road Autonomous Vehicle Standards Committee (part of the Vehicle Engineering Systems Group of the Motor Vehicle Council) embarked on standard setting for "On-Road Autonomous Vehicles" in 2012.[177] Standards for autonomous vehicles are being called for by both industry and legislators.[178] Privacy requirements should be among these standards.

Legislation is also likely to affect interactions between privacy and autonomous vehicles. Privacy issues related to a person's physical location (often called "location privacy") have become highly visible. In response, legislation governing that aspect of autonomous vehicles has already been introduced. Legislation pending before the 112th Congress in 2012 includes both Senator Franken's "Location Privacy Protection Act" (S. 1223) and the "Geolocation Privacy and Surveillance Act" (H.R. 2168 and S. 1212) as well as Senator Leahy's "Electronic Communications Privacy Act Amendments Act of 2011" (S. 1011), of which Section 5

177. *See On-Road Autonomous Vehicle Standards Committee*, *supra* note 65.

178. For example, California State Senator Alex Padilla has introduced SB 1298 to allow autonomous vehicles to be licenseable in California. Chuck Squatriglia, *California Lawmaker Wants Rules for Robo-Cars, Autopia Blog*, WIRED (Feb. 29, 2012, 7:10 PM), http://www.wired.com/autopia/2012/02/padilla-robo-cars-sb-1298.

focuses on "Location Information Privacy." In the Executive Branch, the White House has suggested legislative enactment of the Consumer Privacy Bill of Rights, discussed above, that directly addresses networks and location information both of which are likely to be features of autonomous vehicles.[179]

Proposed legislation likely to affect autonomous vehicles contains a variety of initiatives. These legislative proposals are significant because they all call for protection of location privacy rights of consumers, including those who may become users of autonomous vehicles. For example, Senator Franken's proposed legislation, S. 1223, expressly applies to communications devices, "including but not limited to, a vehicle the individual drives."[180] All of the various legislative proposals regarding location privacy place privacy protection responsibilities on technology providers to assure that potential users retain control over collection of personal location information and affirmatively and knowingly consent before users' personal location information is collected or used. In the future, federal legislation may also specifically regulate autonomous vehicles on a national basis. If so, requirements for privacy protections, as well as privacy impact analyses and regular privacy audits, should be included, as well as limits prohibiting use of autonomous vehicles for surveillance purposes.

As a regulatory matter, the National Highway Traffic Safety Administration (NHTSA) has indicated that the agency understands the importance of privacy, particularly location privacy, with regard to regulating autonomous vehicles.[181] Regulatory measures either in the form of autonomous vehicle safety standards related to consumer acceptance or in response to legislation regarding autonomous vehicles would wisely include specific requirements for protection of autonomous vehicle users' privacy. Since NHTSA considers privacy protection to be an important aspect of consumer acceptance of autonomous vehicles,[182] safety rules regarding autonomous vehicles are should recognize the need not only for technical standards,

179. *See* WHITE HOUSE PRIVACY REPORT, *supra* note 63.
180. Location Privacy Protection Act, S. 1223, 112th Cong. § 3(a) (2011).
181. *See* Wood et al., *supra* note 8, at 1446, 1461–63, 1466–67.
182. *Id.*

but also for privacy policies as well.

Other federal agencies, including both the Federal Trade Commission and the Department of Commerce, have suggested the need for particular measures to protect location information in the context of Internet browsing and mobile devices. The Federal Trade Commission Report, "Protecting Consumer Privacy in an Era of Rapid Change," released in March 2012, expresses specific concern about location-based mobile services.[183] Since that time, FTC has intensified its scrutiny of both on-line Internet tracking and on-the-road location tracking.[184] Concerns about Internet tracking related to online behavioral advertising that records people's movements on the Internet are in some ways similar to concerns about tracking people in real space, including people using autonomous vehicles. In both contexts, user choice and consent are as important as they are difficult to obtain and to maintain. Both on the road and on line, "Do Not Track" should mean, "when the consumer so chooses, Do Not Collect."[185]

Many different privacy-enhancing technologies, such as encryption and anonymization, are available to privacy-minded autonomous vehicle developers. Autonomous vehicles have the potential to apply intelligent systems to make protection of privacy interests automatic. For example, privacy limits (such as transmitting or retaining only anonymous information, or automatic encryption of all personal information) could be built into an autonomous vehicle's technology to prevent privacy problems from arising. Such measures would also reassure autonomous vehicle users, who might otherwise be reluctant to trust autonomous vehicles because of privacy concerns. Autonomous vehicles also could be technically prevented from collecting, storing, or transmitting specific information related to a person, such as the person's location or home address. In other words, the intelligence that drives an autonomous vehicle should be smart enough to make privacy protection part of the

183. *See* FED. TRADE COMM'N REPORT, *supra* note 49.

184. *See, e.g.*, *Id.*; MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DIS*APP*OINTING (2012), *available at* http://ftc.gov/os/2012/02/120216 mobile_apps_kids.pdf.

185. Brill, *supra* note 62.

architecture of autonomous vehicles.

An autonomous vehicle can be designed to minimize personal information that it generates, collects, or retains. Such technical measures as encryption and access controls can also help prevent any personal information that is collected by an autonomous vehicle from becoming available to others. If personal information is necessary to perform a particular function (such as toll payment), that personal information should be automatically destroyed when that transitory purpose (paying the toll) has been accomplished.[186] Autonomous vehicles can also be built to prevent external control from taking over an autonomous vehicle from its user. Measures that permit a user to retain or to regain control over the vehicle would also facilitate autonomy privacy interests of prospective users of autonomous vehicles.[187]

Particular types of autonomous vehicles will likely require attention to different types of privacy enhancing technologies. For example, an interconnected autonomous vehicle will likely transmit significant amounts of information, potentially including personal information. That personal information needs to be rendered anonymous, as well as encrypted, before it is transmitted into the network. Moreover, access to such a network needs to be secured through such controls as changing encryption keys and identifiers. The selfcontained type of autonomous vehicle will also require strict limits on retaining personal information and efforts to protect the anonymity of users. Any recorded personal information would also need to be strongly encrypted, protected by access authentication and subject to tough physical security.

Preventing use of both types of autonomous vehicles from becoming surveillance tools will require political commitment as well as legal enforcement of privacy norms protecting

186. For example, the 511.org traveler information system in the San Francisco Bay area has embraced significant privacy protections. *See Privacy*, 511 SF BAY TRAFFIC, http://traffic.511.org/privacy.asp (last visited Apr. 22, 2012); *see also* Adam Clymer, *Tracking Bay Area Traffic Creates Concern for Privacy*, N.Y. TIMES, Aug. 26, 2002, at A11.

187. For example, a recent article has made a special plea that all autonomous vehicles should have a steering wheel. Jonah Goldberg, *Take the Wheel, Somebody*, NAT'L REV. ONLINE (Mar. 9, 2012, 12:00 AM), http://www.nationalreview.com/articles/293005/take-wheel-somebody-jonah-goldberg.

individuals from potentially overbearing social and governmental systems. Most important, these privacy issues must be systematically addressed in advance—before autonomous vehicles become consumer products.

CONCLUSION

Careful attention both to privacy and to the potential of autonomous vehicles to enhance safety and mobility can generate favorable synergies. Privacy concerns will influence how autonomous vehicles are configured, just as individual privacy and freedom will be affected by the ways in which autonomous vehicles are designed and operated. Infusing privacy into these powerful disruptive technologies will present many challenges, none of them insurmountable. In the end, the future success of autonomous vehicles will depend in part on how well privacy interests and autonomous vehicles can work together. This Article has discussed some ways to make that happen. Now, before consumer versions are offered to the public, autonomous vehicles have a unique opportunity to design privacy into these new modes of personal mobility. After all, autonomous vehicles that deserve the trust and confidence of people who will decide whether or not to use them is a goal shared by both autonomous vehicle developers and those concerned about personal privacy.