Privacy on the Open Road

Professor Dorothy J. Glancy*

30 OHIO NORTHERN LAW REVIEW 295 (2004)

I. Introduction

At a time when enhancement in surveillance technology appears to be matched by the will to use them,[1] it may seem odd to discuss privacy on the open road. But United States law does recognize privacy protections, notwithstanding both the advent of sophisticated surveillance technologies as well as rejection by some of the very idea of any expectation of privacy on the open road.[2] Along the roads and highways of the United States, people traveling from place to place continue to act like they expect a certain degree of privacy.[3] These, perhaps naive, expectations of privacy are a persistent reality despite ever-expanding "automobile exceptions" to federal constitutional protections against unreasonable searches and seizures and court decisions upholding traffic stops. Indeed, lawyers and judges may be more surprised than ordinary people to learn just how many legal protections there are for privacy rights of people on public roads and highways.

These controversial privacy rights on the open road take on added importance as modern surveillance technologies make keeping track of people on public roadways relatively cheap and easy. Roadway surveillance has become nearly ubiquitous, as an array of new technologies, such as Intelligent Transportation Systems (ITS), make possible pervasive, and often covert, tracking of travelers along roads and highways throughout the United States. Some of these ITS systems are designed to collect information about overall transportation patterns and traffic flows. But others, such as automatic vehicle identification (AVI), can target and track specific vehicles and the individuals in them. The ITS archived data user service (ADUS) has the potential to maintain records of where an individual has been in monitored areas.[4] These ITS technologies can pinpoint where a person is. They can connect that location with other records, such as where that person has been in the past. They can even be used to predict the person's future movements and locations. What is unprecedented about ITS technologies is the scale at which they operate. In part because of funding by the federal government,[5] they are almost everywhere. Management of such omnipresent roadway surveillance systems so

---

* Dorothy J. Glancy, Professor of Law, Santa Clara University School of Law. B.A., Wellesley College; J.D., Harvard Law School. Research for this article was supported by a grant from the Center for Science, Technology and Society at Santa Clara University.

[1] *E.g.,* USA PATRIOT Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001), Pub. L. No. 107-56, 115 Stat. 272 (2001), *amended by* Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, 117 Stat. 2599 (2003).

[2] For example, Chief Justice Rehnquist bluntly stated twenty years ago that, "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." United States v. Knotts, 460 U.S. 276, 281 (1983). More recently, even Justice Rehnquist joined in the court's unanimous decision in Illinois v. Lidster, 124 S. Ct. 885, 891 (2004), that holds roadblock and checkpoint stops are seizures for the purposes of the Fourth Amendment.

[3] Activities of drivers in their vehicles - from teeth flossing, to eating, kissing, dressing and undressing, not to mention the ever-popular nose-picking - often seem to reflect expectations that vehicles are private spheres. *See* NATIONAL CONFERENCE OF STATE LEGISLATURES, ALONG FOR THE RIDE: REDUCING DRIVER DISTRACTIONS (2002); LEON JAMES, DATA ON THE PRIVATE WORLD OF THE DRIVER IN TRAFFIC: AFFECTIVE, COGNITIVE, AND SENSORIMOTOR (1984), *at* http://www.soc.hawaii.edui/leonj/leonj/leonpsy/instructor/driving1.html (last visited Aug. 9, 2004). Among the many amusing and frightening newspaper accounts of private behavior in automobiles are: Katie Kerwin McCrimmon, *Driven to Distraction*, ROCKY MOUNTAIN NEWS, June 3, 2002, at 3D; Aly Sujo, *Most Drivers Shred Rules of Road*, NEW YORK POST, May 28, 2003, at 30; *The 7 Car-dinal Sins of the Daily Commute*, THE SHEBOYGAN PRESS, Nov. 21, 2002, at 1C.

[4] AVI and ADUS are types of ITS systems discussed, *infra* notes 27-33.

[5] Federal ITS funding for Fiscal Year 2004 will amount to $232 million, according to the Intelligent Transportation Society of America, *at* http://www.itsa.org/itsnews.nsf/0/ebbdfa05db4142dd85256de9007454a8 (last visited Aug. 9, 2004). All ITS funding since the program's inception in 1991 amounts to an estimated 80.9 billion dollars in capital costs. MELVYN CHESLOW & BARBARA L.

that they do not interfere with privacy rights poses a major challenge to ITS and ITS operators.

Just as ITS and other surveillance tools focusing on roads and highways have become more widely available, concerns about homeland security, thwarting potential terrorist attacks and combating antisocial behavior have stimulated government demand for and use of such on-the-road information for law enforcement and intelligence purposes. Finding and keeping track of potential threats to public order are increasingly important issues. At the same time, in the private sector, real-time and historical information about a person's travel patterns is extremely valuable to "location" marketers and to those engaged in geodemographic[6] marketing of products and services. As Thomas Friedman has suggested, privacy rights can be threatened not only by 1984's "Big Brother" - George Orwell's image of an omnipresent totalitarian government[7] - but also by "little brother," the private-sector information collector.[8] On public roadways, it seems like Big Brother is accompanied by a gang of little brothers, none of whom has any respect for individual privacy. Actually, there are three potential categories of users of information about people on roads and highways: two types of government agencies, in the form of law enforcement and civil transportation authorities, as well as a variety of private-sector marketing and advertising companies. With apologies both to Orwell and to Friedman, one might call these minders of roadway information Big Brother (law enforcement and intelligence agencies), Big Sister (civil transportation authorities) and a heterogenous band of little brothers (private-sector entities such as advertisers, insurers, vehicle manufacturers and the like).

When these three types of roadway information mavens get together to collect and to share surveillance information about the location and travel patterns of individuals, privacy seems at great risk. The Department of Defense's infamous "Total Information Awareness," later reconstituted as "Terrorism Information Awareness,"[9] caused public uproar because of fears that privacy would be compromised by combining government and private information sources. Continuing controversies over the Matrix (Multistate Antiterrorism Information Exchange) program[10] and the Transportation Security Agency's CAPPS II[11] reflect general uneasiness about "data mining" and collaboration between government and private databases containing personal information about the locations and travel patterns of individuals.

Privacy expectations on the part of people on public roadways may be at the outer limits of legally protected privacy rights, particularly when Federal Constitutional rights against unreasonable searches and seizures are at issue. These days, in Fourth Amendment search and seizure cases, privacy rights on a public

---

STAPLES, NATIONAL COSTS OF THE METROPOLITAN ITS INFRASTRUCTURE: UPDATED WITH 2002 DEPLOYMENT DATA 3RD REVISION, at 20, Table 3-7, (Dep't of Transportation, Intelligent Transportation Systems Joint Program Office, Working Paper No. FHWA-OP-03-178, 2003).

[6] *See* Jon Goss, *"We Know Who You Are and We Know Where You Live": The Instrumental Rationality of Geodemographic Systems*, 71 ECON. GEOGRAPHY 171 (Apr. 1995).

[7] GEORGE ORWELL, 1984 (Harcourt, Brace and Co., 1949).

[8] Thomas L. Friedman, *Little Brother*, N.Y. TIMES, Sept. 26, 1999, § 4, at 17; Thomas L. Friedman, *The Hackers' Lessons*, N.Y. TIMES, Feb. 15, 2000, at A27.

[9] *See* DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), REPORT TO CONGRESS REGARDING THE TERRORISM INFORMATION AWARENESS PROGRAM, (May 20, 2003). Congress eventually voted to de-fund the program in the Department of Defense Appropriations Act, 2004. Carl Hulse, *Congress Shuts Pentagon Unit Over Privacy*, N.Y. TIMES, Sept. 26, 2003, at A20.

[10] Jane Black, *One More Slap at a Prying Eye*, BUS. WK. ONLINE, Feb. 6, 2004. Apparently only Florida, Michigan, Connecticut, Pennsylvania, and Ohio continue to cooperate with the program. John Schwartz, *Privacy Fears Erode Support for a Network to Fight Crime*, N.Y. TIMES, Mar. 15, 2004, at C1.

[11] CAPPS II is an updated version of the existing airport screening program, Computer-Assisted Passenger Prescreening System. Richard Behar, *Never Heard of Acxiom? Chances Are It's Heard of You*, FORTUNE, Feb. 23, 2004, at 140. Concerns about the privacy of screening information has caused repeated delays in the launch of CAPPS II. *See, e.g.,* Matthew L. Wald, *Privacy Issue Delays Change in Airport Screening System*, N.Y. TIMES, Feb.13, 2004, at A21. Dan Verton, *Airline Passenger Screening System Faces Deployment Delays: Unauthorized Access Possible, GAO Says*, COMPUTERWORLD, Feb. 16, 2004, at 7.

road rarely seem to be found "reasonable"[12] or "justifiable"[13] or "legitimate"[14] much less, all three.[15] But rarely does not mean never. In fact, the United States Supreme Court has unanimously agreed that stopping vehicles on public roads is a seizure for the purposes of the Fourth Amendment.[16]

Even though the United States Supreme Court insisted in *Katz v. United States*,[17] that the privacy guarantee of the Fourth Amendment "protects people, not places,"[18] expectations of privacy in some places, such as a person's home,[19] seem to be more intuitively obvious than expectations of privacy in other, more public places, such as roads and highways. But that does not mean that expectations of privacy on public roadways are worthy of no legal protection at all. When courts and legislatures recognize privacy rights on public roads and highways, usually the circumstances, such as the procedural context and the facts at issue, are unusual. Moreover, when decision makers decide to protect privacy on the open road, they usually express particular concern about the societal consequences of failing to protect privacy in this setting. Admittedly, highways typically present unusually "hard cases" for protecting privacy on the open road.[20] It is those hard cases, where privacy protections are perhaps least expected, that are the focus of this exploration of privacy on the open road.

The discussion begins by describing some of the surveillance techniques and technologies that can affect the privacy of travelers along public roadways. Then the article turns to examine some of the privacy interests of people on the open road. The next part considers some of the many types of legal rights that protect the privacy of people on public roads or highways. The article concludes by addressing the principle that people on the open road have important rights to freedom from intrusions and interferences with their on-the-road activities.

---

[12] Kyllo v. United States, 533 U.S. 27 (2001). Justice Harlan's concurring opinion in Katz v. United States, 389 U.S. 347, 360 (1967) initiated reasonableness terminology in connection with decisions whether a search has taken place. *Id.*

[13] "Justifiable" was the chosen privacy-expectation modifier in the plurality opinion in United States v. White, 401 U.S. 745 (1971), which also used "reasonable" and "legitimate" as adjectives. *See also* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 616-17 (1989).

[14] Couch v. United States 409 U.S. 322, 336 (1973) (discussing the legitimacy of privacy expectations). *See also* Bartnicki v. Vopper, 532 U.S. 514, 540 (2001).

[15] United States v. Dunn, 480 U.S. 294, 315 (1987). There are, of course, critics of reasonable expectations of privacy analysis. Perhaps the most acerbic is Justice Scalia. Concurring in Minnesota v. Carter, 525 U.S. 83 (1998), a case in which the United States Supreme Court refused to suppress narcotics evidence against visitors to an apartment that was searched without a warrant, Justice Scalia complained that the "reasonable expectation of privacy" test lacks any "plausible foundation in the text of the Fourth Amendment," and is also "self-indulgent." *Id. a*t 97 (Scalia, J., concurring). "[U]nsurprisingly, those 'actual (subjective) expectations of privacy' 'that society is prepared to recognize as 'reasonable,'" he scoffed, "bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable." *Id*. (Scalia, J., concurring) (quoting in part Katz v. United States, 389 U.S. 347, 361 (1967)). *See* discussion of reasonable expectations of privacy, *infra* notes 116-29.

[16] Illinois v. Lidster, 124 S. Ct. 885 (2004).

[17] 389 U.S. 347 (1967).

[18] Katz, 389 U.S. at 351. The place involved in *Katz* was a public phone booth. *Id.* at 348. The Court noted, "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351.

[19] "At the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." Silverman v. United States, 365 U.S. 505, 511 (1961). In Kyllo v. United States, 533 U.S. 27 (2001), a case involving infrared monitoring of a home, Justice Scalia writing for the majority put the matter somewhat more directly by stating, "With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." *Id.* at 31.

[20] The concept of "hard cases" comes from RONALD DWORKIN, TAKING RIGHTS SERIOUSLY 81-130 (1977).

II. Tracking Techniques and Technologies

Watching people travel on public roads is often described as "fair game,"[21] an age-old pastime for anyone who wants to look at the passing scene.[22] Indeed, people tracking other people as they move from place to place seems to be about as old as humanity.[23] Even non-human animals track other animals, often seeking to prey on them.[24]

There are many ways to keep track of a person (a target, in surveillance terms) as he or she moves about in the physical world. Having other people physically follow a targeted individual wherever the latter goes is one, fairly low-tech, way of tracking a targeted person.[25] Investigators sometimes call this type of visual surveillance "tailing" or "shadowing." But such physical following has practical drawbacks, in addition to its intrusion on the privacy of the person being followed. First, physical surveillance is expensive in terms of person-time, usually requiring at least one follower (often several followers) for each person being followed. Second, once the person being followed realizes that she is being followed, she usually reacts by either eluding or attacking her trackers. On top of these logistical problems, keeping track of both the present and all of the past locations of a tracked person in readily retrievable and interrelateable form can pose significant information-management challenges. These practical problems tend to limit the use of physical surveillance to very few targets.

Advances in technology now make it possible to target and track many more people - in fact, nearly everyone on a road or highway. New surveillance technologies greatly expand capacities to keep track of large numbers of people both in real time and historically over time.[26] Several attributes of modern roadway

---

[21] There are, of course, instances of illegal stalking - actively following someone in a manner to cause fear. The crime of stalking is discussed *infra* note 208.

[22] For example, one of Edgar Allan Poe's most enigmatic stories is *The Man of the Crowd* from his TALES OF THE GROTESQUE AND ARABESQUE (1840). In Poe's story, an anonymous observer/voyeur describes how he became fascinated by an elderly man with "a countenance which at once arrested and absorbed my whole attention, on account of the absolute idiosyncracy of its expression." In the end, the observer concludes that the old man is "the type and the genius of deep crime. He refuses to be alone. *He is the man of the crowd*. It will be in vain to follow, for I shall learn no more of him, nor of his deeds." EDGAR ALLAN POE, COLLECTED WORKS OF EDGAR ALLAN POE, 506, 515 (T.O. Mabbott, ed., Belknap Press, 1969) (emphasis added).

Examples of current books about people-watching range from Dr. Aaron W. Wolfgang's EVERYBODY'S GUIDE TO PEOPLE WATCHING (1995) to ROUTE 66: THE HIGHWAY AND ITS PEOPLE (1988) by Susan C. Kelly and Quinta Scott. The popularity of webcams and reality video also reflects the human fascination with watching other humans.

[23] H.T. Bunn & E.M. Kroll, *Systematic Butchery by Plio/Pleistocene Hominids at Olduvai Gorge, Tanzania*, 27 CURRENT ANTHROPOLOGY 431-52 (1986); RICHARD B. LEE & IRVEN DEVORE, MAN THE HUNTER (1969); ROBERT W. SUSSMAN, THE BIOLOGICAL BASIS OF HUMAN BEHAVIOR (2d ed. 1998); LAURA BETZIG, HUMAN NATURE: A HUMAN EVOLUTION 329 (1989); J.D. Speth, *Early Hominid Hunting and Scavenging*, 18 JOURNAL OF HUMAN EVOLUTION 329 (1989). *Cf.* Craig. B. Stanford, *Chimpanzee Hunting Behavior and Human Evolution*, AMERICAN SCIENTIST (May-June 1995).

[24] Among the species most closely studied for their hunting patterns are Chimpanzees. Stanford, *supra* note 23.

[25] Nineteenth century Native Americans were famous for their tracking skills. Kenneth W Porter, *The Seminole-Negro Indian Scout, 1870-1881*, 55 SW. HIST. Q. 358 (1951). The legendary Apache Scouts may have been among the most expert trackers in American history. *See* Eve Ball, *The Apache Scouts: A Circicahua Appraisal*, 7 ARIZ. & THE WEST 315 (1965).

[26] Technologies that project surveillance in unseen and unanticipated ways have long concerned the courts. For example, Justice Scalia's opinion for the Court in Kyllo v. United States, 533 U.S. 27, 31 (2001) held that thermal radiation scanning (a "technological enhancement or ordinary perception") of a home from a public street constitutes an unreasonable search for the purposes of the Fourth Amendment. His opinion for the Court concludes by stating, "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion' . . . constitutes a search" under Silverman v. United States, 365 U.S. 505 (1961). *Id.* at 34. Justice Scalia explained that when "the technology in question is not in general public use," it is necessary to treat its use as a search. *Id.* After all,"preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted" is what is at stake. *Id.* His concern was, of course, not about roadways but about leaving "the homeowner at the mercy of advancing technology." *Id.* at 35. This article suggests that there should be similar concerns about leaving people on roads and highways "at the mercy of advancing technology," in the form of the new types of surveillance technology discussed in this article.

surveillance technologies enhance their effectiveness. First, many of the new surveillance technologies tend to be discrete to the point of virtual invisibility, so that people tracked by them usually have no way of knowing that they are being tracked. Second, use of these surveillance technologies is widespread. In part because of federal funding for Intelligent Transportation Systems (ITS), United States roads and highways are increasingly covered by traffic surveillance.[27] Third, the emphasis on nationwide interoperability of ITS surveillance systems, together with use of digital formats for data collection, make roadway surveillance information widely available, interchangeable and manipulable through searchable relational databases. Some of these databases contain real-time location information. Some databases are historical - retaining archives of the times and places of past travel patterns. Others are used to model and predict future travel. Fourth, because digital location data is often cheaper to retain than to edit or to destroy, roadway surveillance information may be kept indefinitely. In the near future, ITS systems will potentially be able to collect information everywhere about everybody's and anybody's whereabouts all the time.

Some of the legal restrictions on use of these high-tech tracking systems will be the focus of Part IV. At this point, it is important to consider some of the many types of modern surveillance technologies that can be deployed along roads and highways both by ITS systems and private-sector entities, as well as by law enforcement.

Intelligent Transportation Systems

Much of the ITS infrastructure is funded and managed by government transportation agencies - mostly at the regional or local level - with funding coming primarily from the United States Department of Transportation (USDOT).[28] In operation, ITS systems comprise a wide array of both public and private projects, as well as public-private partnerships. On occasion, law enforcement agencies participate in particular ITS projects; but law enforcement is virtually never the lead agency that manages such projects.

ITS technologies are beginning to make pervasive electronic surveillance of people along roads and highways a reality. They include various types of two-way transponders, remote cameras, license plate readers, as well as diagnostic systems and location devices that keep track of the movement and locations of wireless communications and the wireless devices themselves. When two-way telecommunications devices are built into a vehicle, such systems are called telematics. Other types of wireless communication devices, such as cellular telephones, data messaging systems and personal digital assistants, although not integrated into vehicles, can nonetheless be used to keep track of a person's location both in real time and on an historical basis. Together, these technologies can relentlessly track almost anyone or anything that moves on public roads and highways.

As a general matter, ITS does not always or necessarily involve roadway surveillance.[29] Originally called Intelligent Vehicle Highway Systems (IVHS), ITS technologies were initially designed to be impersonal, in that they focused on anonymous vehicles in relationship with highways, rather than on identifiable individuals in vehicles or along roadways.[30]

The United States Department of Transportation (USDOT), primarily through the Federal Highway Administration, has provided billions of dollars of funding for ITS projects. But USDOT generally does not micromanage particular ITS systems much less encourage targeted surveillance. The ITS Joint Program Office

---

[27] An estimated 80.9 billion dollars in capital costs have been invested in ITS systems since these systems were launched as part of ISTEA 1991. CHESLOW & STAPLES, *supra* note 5.

[28] Within USDOT, ITS projects are usually managed through the Joint Program Office for Intelligent Transportation Systems.

[29] The range of ITS activities is suggested by the 33 types of technologies, divided into eight user services, bundles included within the National ITS Architecture (Version 5.0, April 2004), *at* http://www.its.dot.gov/arch/arch.htm (last visited Aug. 9, 2004). For a complete listing of the 33 types of technologies see Version 5.0 of the National ITS Architecture, *at* http://www.iteris.com/itsarch/html/user/userserv.htm (last visited Aug. 9, 2004).

[30] *See* Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 SANTA CLARA COMPUTER & HIGH TECH. L. J. 151 (1995). This study considered an earlier version of ITS architecture which was somewhat less involved in surveillance.

within USDOT is currently in charge of most ITS matters for USDOT.

On-the-ground ITS projects are typically under the control of local or regional transportation authorities. Sometimes these local or regional agencies partner with other public agencies, including law enforcement, as well as private companies. The TravInfo ITS project in the San Francisco Bay Area is typical. It is a joint project of the region's Metropolitan Transportation Commission (MTC), CalTrans (the California state department of transportation) and the California Highway Patrol.[31] A private-sector company, PB Farradyne, Inc. designed and manages TravInfo for the Metropolitan Transportation Commission and its partners.[32] The purpose of the TravInfo ITS project is to gather and provide traffic information in the San Francisco Bay area with a view toward improving transportation efficiency, reducing environmental consequences of congestion and promoting highway safety.

Initially ITS surveillance technologies collected aggregate information about traffic flows, such as the rate of use of a segment of highway or of an on-ramp or off-ramp to a bridge or tunnel, rather than personal data related to a particular traveler or vehicle. However, over time, as ITS programs began to focus increasingly on transportation users and their personal activities, a greater emphasis on targeting individuals began to emerge. Today a number of ITS technologies collect and manage individualized location information and origin-destination data, such as the commute pattern of a person traveling from her home to her workplace and back. Although surveillance of individuals is nowhere listed as an ITS function or user service, many ITS technologies focus on individual travelers' activities and locations. ITS applications can track the locations a traveler visits and maintain itineraries of an individual's past travel. These applications, and the data collected by them, are sometimes even used to predict the individual's future movements and activities.[33]

---

[31] *See* the Metropolitan Transportation Commission website, *at* http://www.mtc.ca.gov/projects/travinfo/travinf1.htm (last visited Aug. 9, 2004); 511 Traffic website, *at* http://traffic.511.org/traffic_partners.asp (last visited Aug. 9, 2004).

[32] *See* press release regarding the TravInfo project on the Metropolitan Transportation Commission website, *at* http://www.mtc.ca.gov/whats_happening/press_releases/rel107.htm (last visited Aug. 9, 2004).

[33] More than half of the 33 ITS user services appear to contemplate collection of data about identifiable individuals. These user services include:

1. Travel And Traffic Management User Services
1.1 Pre-trip Travel Information
1.2 En-route Driver Information
1.3 Route Guidance
1.4 Ride Matching And Reservation
1.5 Traveler Services Information
1.7 Incident Management
1.8 Travel Demand Management
1.9 Emissions Testing And Mitigation

2. Public Transportation Management User Services
2.3 Personalized Public Transit
2.4 Public Travel Security

3. Electronic Payment User Services
3.1 Electronic Payment Services

4. Commercial Vehicle Operations User Services
4.1 Commercial Vehicle Electronic Clearance
4.2 Automated Roadside Safety Inspection
4.3 On-board Safety and Security Monitoring
4.4 Commercial Vehicle Administrative Processes

5. Emergency Management User Services
5.1 Emergency Notification And Personal Security
5.2 Emergency Vehicle Management

Traffic Cameras

Video cameras that capture moving and still images of roadways and the people and objects on them represent some of the most common ITS surveillance technologies. Among the most widely used are remotely operated closed-circuit television cameras located high above roadways, often discretely placed so that they are difficult to see from the roadway. These unobtrusive traffic cameras are usually operated and monitored by a traffic management center located some distance away from the camera and the highway being surveiled. The traffic management center operator has pan-zoom-tilt remote controls that permit the operator to pan along a highway, zoom out to look at the general traffic landscape or tilt down and zoom in to closely monitor particular locations (bridges, tunnels, on-ramps and off-ramps) or incidents (accidents or bottlenecks). Local television stations often broadcast real-time wide-angle views from such cameras showing traffic flows, or traffic jams. These real-time images of roadways are also popular places on the websites of transportation agencies. In addition to television cameras, still cameras can be installed at specific locations, such as at entrances to parking facilities or airports, at intersections or even along highways. These still cameras automatically capture a digital image of each vehicle that passes the camera.

When these cameras are used to focus on particular vehicles, they are part of a group of ITS technologies known as Automated Vehicle Identification (AVI). For example, in many states still cameras automatically take digital pictures of vehicles, and their drivers, that run red lights (red light runner cameras) or exceed the speed limit (photo radar). These digital pictures are often enhanced by license plate recognition, discussed below. In the future, facial recognition software, that takes a digital image of a person's face, even through a windshield, and compares it against a database of persons of interest to law enforcement may also become a common feature of digital cameras along roadsides.

When a traffic camera focuses in on an individual person, for example by capturing an image of the face of a driver or passenger, the privacy of the individual photographed is at stake. Remote television and still cameras can also scrutinize pedestrians walking alongside a roadway, as well as bicyclists, bystanders or people on sidewalks. Higher resolution cameras can capture what an individual is doing, her apparent emotional state, who accompanies her, what she is carrying or what she is reading. Moreover, traffic cameras with remote control functions can permit unseen operators to capture images of the faces and activities of people in nearby buildings, in addition to information about anonymous traffic flows and persons on or near the roadway.[34]

License Plate Recognition

Automatic license plate recognition is a specialized ITS application of digital cameras. It is also a type of automatic vehicle identification (AVI). A license plate reader takes a digital picture of a license plate, computerizes it and then compares it against a database of license plate numbers and letters associated with particular vehicles and their owners.[35] Often the digitized version of the numbers and letters on a license plate is stored for later comparison with similar digitized data captured at other times and places. License plate recognition is used for a variety of traffic management, weigh-in-motion commercial vehicle inspections, security, parking, border control and other purposes. In the United Kingdom, the recently adopted system for reducing traffic congestion in London relies on license plate recognition as the basis for charging vehicles to

---

7. Information Management User Services

7.1 Archived Data Function

Version 5.0 of the National ITS Architecture, *at* http://www.iteris.com/itsarch/html/user/userserv.htm (last visited Aug. 9, 2004).

[34] A California statute makes it illegal to use such cameras to peer into the privacy of a person's home. CAL. CIV. CODE § 1708.8. (West Supp. 2004).

[35] The website of Hi-Tech Solutions, a company that specializes in advance image processing, demonstrates the operation of license plate recognition, *at* http://htsol.com (last visited Aug. 9, 2004).

enter central London during peak hours.[36]

From the perspective of privacy law in the United States, license plate recognition is interesting because most of the decisional law regarding license plates has not considered a license plate to be private information. The argument is that a license plate cannot be private because it is after all affixed to the exterior of the vehicle where it can be seen by whomever wants to take notice.[37] However, in France, the European Data Union's Protection Directive[38] has been interpreted to protect the privacy of a person's license plate number.[39]

Toll Tag Transponders

A different type of ITS automatic vehicle identification uses toll tags, an increasingly common device used to pay tolls along United States roadways, also to provide traffic surveillance.[40] Toll tags are transponders, usually smaller than a deck of cards, that are capable of rudimentary two-way communication. Most toll tags are voluntarily installed on the windshields of vehicles by drivers who pass through tag-readers at toll collection points and use their tags to automatically pay tolls for use of highways, bridges and tunnels. Electronically, a toll tag is a simple two-way radio transmitter programmed to respond to an activation signal with specific information - typically the transponder's unique numeric identifier.[41] In most toll tag systems, the transponder remains the property of the toll collection agency and is licensed for use by drivers. In its toll collection function, the tag is automatically identified each time it passes close to a transponder-reader at a toll collection facility. The toll tag reader uses the tag identification to deduct the toll amount from what is usually a prepaid "debit" account. The Transportation Corridor Agencies in Southern California have also arranged for the use of the toll tags to pay for purchases at McDonald's restaurants. Other toll tag purchasing opportunities are planned

---

[36] The London system, called "Congestion Charging," has its own website, *at* http://www.cclondon.com (last visited Aug. 9, 2004). This site even includes a Privacy Policy. *See also*, Georgina Santos, *Road Pricing on the Basis of Congestion Costs: Consistent Results from Two Historic UK Towns* (July 1999) (unpublished manuscript, *at* http://www.econ.cam.ac.uk/dae/people/santos/trb2000.pdf (last visited Aug. 9, 2004).

[37] Typical court decisions denying any reasonable privacy expectation in a license plate include: United States v. Walraven, 892 F.2d 972, 974 (10th Cir. 1989); State v. Bjerke, 697 A.2d 1069 (R.I. 1997); State v. Myrick, 659 A.2d 976 (N.J. Super. Ct. Law Div. 1995).

[38] Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L281).

[39] Déliberation no. 96-069 du 10 septembre 1996 relative à la demande d'avis portant création à titre expérimental d'un traitement aautomatisé d'informations nominatives ayaant pour finalité principale la lecture automatique des plaques d'immatriculation des véhicules en movement par la société des autoroutes Paris-Rhin-Rhône (SAPR). This ruling is discussed in JOEL R. REIDENBERG & PAUL M. SCHWARTZ, DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES 32 (2002), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/studies/regul_en.pdf (last visited Aug. 10, 2004).

[40] About twenty types of electronic toll collection systems are in use, mostly for bridge and highway toll collection, in dozens of places around the United States.

[41] Federal Communications Commission regulations regarding these devices are published at 47 C.F.R. § 15.251 (1989) under the category, "Automatic Vehicle Monitoring." These regulations may change with the adoption of the new ITS DSCR standards, discussed *infra*. *See* IN THE MATTER OF AMENDMENT OF THE COMMISSION'S RULES REGARDING DEDICATED SHORT-RANGE COMMUNICATION SERVICES IN THE 5.850-5.925 GHZ BAND (5.9 GHZ BAND); AMENDMENT OF PARTS 2 AND 90 OF THE COMMISSIONS RULES TO ALLOCATE THE 5.850-5.925 GHZ BAND TO THE MOBILE SERVICE FOR DEDICATED SHORT RANGE COMMUNICATIONS OF INTELLIGENT TRANSPORTATION SERVICES, Release Number FCC 03-324 (adopted Dec. 17, 2003; released Feb. 10, 2004) [hereinafter FCC 03-324], *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-324A1.pdf (last visited Aug. 10, 2004).

- such as for parking, car washes, automotive products such as gasoline and oil, as well as many other types of goods and services.

Although toll tags can have several different technical formats, they are designed to be generic, with an open architecture available to all. For example, technical specifications for transponders used in California are published in the California Code of Regulations title 21 sections 1700 -1705.8. Any unshielded toll tag within range of a transponder reader can be addressed to respond with the device's unique identifier.[42] So it is possible to follow the successive locations of transponders, and the vehicles to which these devices are attached, as they move past toll tag readers located at places along roads and highways, as well as at toll collection facilities. The TravInfo ITS project of the Metropolitan Transportation Commission in the San Francisco Bay Area has found that a network of such toll tag readers is a useful way to collect information about traffic flows, volumes and speeds.[43]

There is no immediate connection between a toll tag's unique identifier and any particular vehicle or person. But the toll tag issuer typically associates the unique identifier with the name, address and other information regarding the licensed toll tag holder, as well as all vehicles in which the toll tag may be used and the drivers who may drive those vehicles.[44]

Vehicle Black Boxes

It is estimated that forty million vehicles in the United States[45] already have built into them event data recorders, or "crash data recorders." These computerized diagnostic modules are informally called "black boxes," after flight data recorders in airplanes. In the future, such equipment is expected to become mandatory on all new vehicles sold in the United States.[46] Modern vehicles usually have several computer modules that automatically sense and record vehicle behavior, speed, mechanical operation, emissions, seat-belt use, and the like. A typical Black Box is one of those modules - a critical-event module designed to collect information about a vehicle in the seconds before the vehicle's airbags deploy.

Many drivers know that their automobiles are equipped with expensive-to-repair computers. But they usually do not know, because manufacturers do not often disclose it, that within the vehicle's computer system is an event data recorder, or critical-event module, designed to automatically capture the driver's speed, driving patterns, seatbelt use, and the mechanical status of the vehicle at the time of an accident. Vehicle manufacturers

---

[42] California Code of Regulations title 21 section 1703(I) provides for a " 32-bit code [that] uniquely identifies which transponder is responding to a polling request or is being acknowledged." CAL. CODE REGS. tit. 21, §1703(I). Addressing a toll tag transponder is called "pinging" the transponder.

[43] *See* the Metropolitan Transportation Commission website, *at* http://www.mtc.ca.gov/projects/travinfo/travinf1.htm (last visited Aug. 9, 2004).

[44] It is interesting to contrast the user agreements of various toll collection agencies. For example, when the state department of transportation, Caltrans, issues a toll tag, it is accompanied by a Personal Information Notice that notes restrictions on disclosure of information provided in the application for a toll tag. However, other issuers, such as bridge districts and private-sector toll road agencies, do not promise such non-disclosure of the information collected in the application and licence agreement for their toll tags.

[45] Ed Garsten, *Auto "Black Boxes" Defended*, DETROIT NEWS, Nov. 20, 2003, at 1B. These crash data recorders are standard equipment on General Motors vehicles, as well as some Ford models and those of a number of other manufacturers.

[46] They are already required on busses and commercial vehicles, and are under active consideration as required equipment in all vehicles. Most black boxes in use in the United States are manufactured by Vetronix. *See* Vetronix website, *at* http://www.vetronix.com/main.html (last visited Aug. 10, 2004).

and insurance companies routinely have diagnosticians download data from these modules for use in analyzing the causes of accidents and assessing legal liability.

The legal issues regarding who owns and has control over the event data collected by a vehicle's Black Box remains unresolved in most of the United States, except California. In 2003 California enacted a statute, California Vehicle Code section 9951, which provides that, as of July 2004, car manufacturers must disclose information about the event data recorders in owner's manuals. Moreover, the statute makes clear that the data contained in the black box is owned by the car owner. Anyone else who wishes to access the event data must secure the consent of the car owner or subpoena the data.[47]

In the future, whether a vehicle is speeding or its driver is wearing a seatbelt may be automatically communicated to an array of roadside receivers using the dedicated short range communications technology described below.[48] Since ITS industries have already developed adaptive systems such as airbags that sense the height and weight of vehicle occupants and then modify the operation of airbags for persons of short stature, such as children, all sorts of diagnostic information might be transmitted. For example, an engineer has patented an in-car system that weighs dieters and counsels them when and what to eat.[49] Such a system could be connected to vehicles's wireless communication systems for transmission to the roadside receiver units described below.

Global Positioning Systems (GPS)

A number of ITS systems that involve keeping track of the locations of vehicles as they move across the physical landscape rely on Global Positioning Systems (GPS).[50] GPS is a highly accurate positioning and navigation technology using a constellation of United States government satellites. There are 24 GPS satellites equipped with atomic clocks in 12-hour orbits 12,000 miles above the earth. Each satellite constantly transmits the precise time and the satellite's position in space. From the ground, between five and eight satellites can be seen from any place on earth.

A vehicle equipped with a GPS receiver uses four satellites to compute four dimensions of position and time to determine the vehicle's location, as well as its speed and direction. Standard Positioning systems can locate a vehicle within 100 meters. More accurate positioning is available through Differential GPS that can locate the vehicle within 1 meter. Differential GPS makes use of a differential signal broadcast from a base station that corrects for inaccuracies caused by the satellite signal's passage through the atmosphere. Dual differential GPS is capable of locating a GPS receiver within one or two centimeters.[51] GPS can locate a vehicle for a variety of vehicle-based telecommunications functions, including telematics and dedicated short range communications as well as other types of mobile communications. Each of these communications-related technologies will be discussed below. Law enforcement use of GPS devices will be discussed in the next section.

Telematics

Telematics refers to vehicle-based mobile telecommunications systems, associated with ITS. Broadly

---

[47] CAL.VEH. CODE § 9951 (2003), discussed *infra* notes 321-23.

[48] *See* text *infra* note 59.

[49] Sabra Chartrand, *Patents: An In-car System for Dieters That Weights Them and Tells Them When They Have Strayed*, N.Y. TIMES, Dec. 29, 2003, at C8.

[50] There are other ways to keep track of the locations of vehicles such as the cellular telecommunications triangulation described *infra* note 61.

[51] CHRIS DRANE & CHRIS RIZOS, POSITIONING SYSTEMS IN INTELLIGENT TRANSPORTATION SYSTEMS (1998). *See also* NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, A TECHNICAL REPORT TO THE SECRETARY OF TRANSPORTATION ON A NATIONAL APPROACH TO AUGMENTED GPS SERVICES (1994), *available at* http://www.itsdocs.fhwa.dot.gov//JPODOCS/REPTS_TE/1r01!.PDF (last visited Aug. 10, 2004).

speaking, telematics enables vehicles, infrastructure such as toll facilities, and travel information providers to communicate with each other. Most telematics systems depend on GPS to locate the telematics user for the purposes of information services, although telematics may make use of any of a wide range of different types of wireless communications. Location-based information services include navigation assistance, internet access, localized real-time traffic and weather reports, travel information about nearby food, lodging and other services, as well as entertainment, such as satellite radio or on-line karaoke. Some of telematics' navigation and travel information systems also use advanced geographical information systems (GIS) such as digital map technologies to provide directions and location assistance. The movements of telematics-equipped vehicles can be tracked by traffic managers and compared with historical data about traffic flows to assess real-time traffic conditions such as slow speeds due to congestion.[52] In some areas, parents use telematics to keep track of teenage children while the latter are driving.[53]

Perhaps the best known of the telematics systems, because it is so widely advertised in the United States, is OnStar by General Motors. OnStar provides emergency roadway assistance as well as travel information through wireless voice communications with a central OnStar monitoring station. OnStar and other systems, such as Networkcar and Vetronix, connect telematics functions with internal diagnostic features of vehicles.[54] The OnStar website describes telematics technology as providing "a broad and evolving array of safety, security, convenience and communications services that are delivered using on-board vehicle electronics, wireless telecommunication technologies, the Internet and global positioning satellite location information."[55]

OnStar Privacy Principles detail OnStar's gathering of personal information: "When you use the OnStar services, we may routinely collect information, such as the automatic network numbering information provided via the telephone network (Caller-ID information), the location of your vehicle provided by satellite and GPS electronics, or any other information, including your preferences or usage patterns."[56] At the end of its Privacy Principles, OnStar offers the following assurance: "You take privacy seriously, and so do we at OnStar. It's our way of sustaining your trust in OnStar and our products and services. After all, your trust is what we value most."[57] But in the fine print, the OnStar Privacy Principles note that:

> While OnStar is committed to protecting your privacy, we cannot guarantee that your private communications and other personally identifiable information will never be disclosed in ways not described in this policy. Subscribers are cautioned that the privacy of any information sent via wireless cellular communications will not be assured. Third parties may, for instance, unlawfully intercept or access transmissions and private communications without our consent. In addition, OnStar may disclose personal information if required to do so by law on in [sic] the good faith belief that such disclosure is reasonably necessary to (i) comply with the legal process, (ii) respond to claims of a violation of the rights of third parties, or (iii) protect the rights, property or safety of OnStar, our users or the public. OnStar cannot accept any responsibility for accidental or inadvertent disclosure, unauthorized access or for other disclosure as required by

---

[52] Tim Moran, *Going with the Flow; Telematics-equipped Vehicles Feed Real-time Information to Highway Systems*, AUTOMOTIVE NEWS, Sept. 23, 2002, at 24T.

[53] Joe Ledford, *Parents Bug Cars to Track Teens*, ATLANTA J. & CONST., Dec. 21, 2002, at 1A.

[54] *Remote Diagnostics--the Next OEM Frontier*, 16 THE HANSEN REP. ON AUTOMOTIVE ELECTRONICS, Dec. 2003/Jan. 2004, at 1.

[55] OnStar Privacy Principles located on the OnStar website, *at* http://www.onstar.com/us_english/jsp/gl_terms_privacy.jsp?page=gl_privacy.jsp (last visited Aug. 10, 2004).

[56] *Id.*

[57] *Id.*

law or described in this policy.[58]

OnStar is fairly typical with regard to the types of information used in its telematics services. It is somewhat unusual in expressing concern about the privacy of telematics users.

Dedicated Short Range Communications (DSRC)

A Federal Communications Commission (FCC) Report and Order released in February 2004 is likely to enhance and expand telematics in the United States. The FCC Order allocates to Intelligent Transportation Systems radio frequencies between 5.850 and 5.925 GHz and adopts the ASTM E2213-03 (ASTM-DSRC) communications standard that extends wi-fi (IEEE standards 802.11 and 802.11a) to vehicles traveling at high speeds.[59] These DSRC communications involve On-board Units (OBUs) associated with GPS automatic location equipment. OBUs are designed to be carried in moving vehicles. The FCC rule contemplates both communications between OBUs in nearby vehicles and communications between OBUs and Roadside Units (RSUs) located along roads and highways.

Most OBUs will be built into vehicles, although portable versions are also contemplated in the form of digital assistants and even smart tags on products and packages. In fact, the United States Department of Transportation has for some time considered requiring OBU devices as standard equipment on all vehicles sold in the United States. An OBU is a two-way radio transceiver, built into or carried in a vehicle. The OBU is designed to communicate automatically with DSRC-equipped roadside units as well as with other vehicles equipped with OBUs. Automatic communications between vehicles equipped with OBUs will enable automatic crash avoidance and automatic warning of dangerous lane changes before one vehicle changes lanes into the path of another on-coming vehicle. The FCC rule also appears to contemplate a variety of other short-range communications between vehicles over an open wi-fi band. OBUs will not require special FCC licenses, so long as they are interoperable with the 802.11-based communication standard adopted for ITS.

RSUs located along roadways will communicate with OBUs through antennas located up to 45 feet above the roadway. RSUs will be licensed on a non-exclusive basis for a geographic area, on a first-come first-served basis. RSU transmitters are allowed to have up to 30 watts of power and the capacity to send and receive communications from about 5 feet to about 3,000 feet. Nationwide licenses will be available, but only for designated geographic areas that are claimed in a particular RSU registration. Public safety communications will have priority; but bandwidth will be available to commercial RSUs in the order of their registrations with the FCC. Although the FCC claims that roadway safety is the main motivation for the ITS DSRC allocation, commercial applications, including a wide variety of telematics services, such as location-based commerce and travel services, are likely to bring location-specific advertising and travel information into OBU-equipped vehicles. OBUs will also be associated with payment systems so that they will ultimately replace toll tags for access to toll facilities and for other payment purposes.

Among the interesting features of the FCC's authorization of DSRC for ITS is the absence of any mention of standards or controls with regard to the privacy or security of the information transmitted. Right now this new vehicle-centered application of wireless communications technology is intentionally wide open to the development of competing systems. However, that very openness can pose risks, such as intrusion and misuse of personal information, that affect the privacy of people who use vehicles equipped with OBUs.

Wireless Communications

Highly popular and not limited to use on the road, wireless mobile telecommunications are essential components of existing vehicle-based telematics. Independently of telematics, cellular telephones, wi-fi and bluetooth devices are frequently used by drivers and pedestrians. An invisible function of these wireless telecommunications devices is their legally required capacity to pinpoint the location of each mobile

---

[58] *Id.*

[59] FCC 03-324, *supra* note 41.

telecommunications device.

The Wireless Communications and Public Safety Act of 1999 designated "911" as the nation-wide emergency telephone number for wireless, as well as wireline, telephones. That statute also contained an E911 mandate requiring wireless carriers to be able to locate wireless 911 callers for emergency services purposes.[60] FCC regulations require wireless carriers to have 95 percent of their subscribers using location-capable handsets (either by incorporating GPS in handsets or by network-based triangulation) by December 31, 2005.[61] The resulting information about the location of wireless communications users is called Automatic Location Information (ALI). ALI is to be used by wireless carriers for making automatic connections between a located wireless device and emergency services. ALI is also available to law enforcement under the Communications Assistance for Law Enforcement Act, 18 U.S.C. § 2522 and 47 U.S.C. §§ 229, 1001-1010[62] as modified by the USA PATRIOT Act.[63] Legal restrictions on the use of this location information derived from wireless telecommunications are discussed below.[64]

Data Archives

The potential for storing itineraries of the locations to and from which a person has traveled in the past is embraced by one of the newer ITS user services - Archived Data User Service (ADUS).[65] Transportation planners use origin-destination information to predict future transportation demands in designing highways and public transit systems. But marketing companies also use such information to predict future travel and purchasing decisions. Moreover, advertisers use such information to construct profiles for targeted advertising. ITS Archived Data User Services are designed to collect and retain transportation data for longitudinal studies of traffic patterns regarding particular locations or transportation segments over time. At present, ADUS technologies do not focus on collecting and storing individual itineraries of particular persons.

But there is likely to be demand, backed by substantial financial resources, for such individualized travel-pattern information in the future. Marketing organizations would find archives of individualized information highly valuable in consumer profiling. Divorce lawyers have already indicated keen interest in such historical data. Law Enforcement agencies also will be likely to find such archived itineraries useful, for example, in placing a suspect at or near the scene of a crime. Moreover, intelligence agencies may seek such information for homeland security purposes. For example, archives of individual data derived from ITS systems would be a highly sought-after component of such data aggregation efforts as TIA or CAPPS II,

---

[60] 47 U.S.C. § 251(e) (2001).

[61] 47 C.F.R. § 20.18(g)(1)(v) (2003). These regulations require location accuracy to be better than 300 meters for almost all calls, and better than 150 meters for two-thirds of all calls.

[62] Cell phone records have been successfully used as evidence in criminal cases. *See, e.g.,* United States v. Forest, 355 F.3d 942 (6th Cir. 2004).

[63] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[64] *See* discussion in text *infra* notes 302-11.

[65] According to the ITS National Architecture 5.0, Section 7.1 ADUS data is managed by an Archived Data Management System that "collects, archives, manages, and distributes data generated from ITS sources for use in transportation administration, policy evaluation, safety, planning, performance monitoring, program assessment, operations, and research applications. The data received is formatted, tagged with attributes that define the data source, conditions under which it was collected, data transformations, and other information (i.e. meta data) necessary to interpret the data. The subsystem can fuse ITS generated data with data from non-ITS sources and other archives to generate information products utilizing data from multiple functional areas, modes, and jurisdictions. The subsystem prepares data products that can serve as inputs to Federal, State, and local data reporting systems. This subsystem may be implemented in many different ways. It may reside within an operational center and provide focused access to a particular agency's data archives. Alternatively, it may operate as a distinct center that collects data from multiple agencies and sources and provides a general data warehouse service for a region." Archived Data Management System, ITS National Architecture 5.0, *at* http://www.iteris.com/itsarch/html/entity/adms_b.htm (last visited Aug. 10, 2004).

discussed above.[66]

Law Enforcement Surveillance Technologies

For a long time, law enforcement agencies have used an array of surveillance techniques in their efforts to find, catch and convict criminal suspects.[67] These surveillance techniques, used both for criminal law enforcement and for intelligence purposes, include physical tracking on the ground or by aircraft. On the technological side, probably the most frequently used law enforcement surveillance technology is the electronic tracking device, actually a group of technologies that includes "beepers" and related devices, such as GPS. Recently, law enforcement has begun to use automatic location information from wireless telecommunications, as well. Most of these technologies are designed to facilitate tracking a target who remains unaware of being tracked. Two other law enforcement tracking technologies, photo radar and photo red light, are often used openly to deter traffic violations such as speeding and running red lights.

Electronic Tracking Devices

Federal electronic surveillance laws describe an electronic tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[68] The Senate Report explains the use of electronic tracking devices, such as beeper transponders, which the Report defines as:

> one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such "homing" devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.[69]

Because they do not intercept the content of communications, electronic tracking devices are exempt from most restrictions on law enforcement use of electronic surveillance.[70] Rather they are governed by 18 U.S.C. § 3117, which provides for warrants authorizing the installation and monitoring of electronic tracking devices.[71]

---

[66] *See* text *supra* notes 10-12.

[67] Before the advent of the automobile, law enforcement agents and agencies hunted down highwaymen and bandits who made surface transportation difficult and dangerous. *See, e.g., The Highwayman's Case (Everet v. Williams)*, 35 L. Q. REV. (July 1893), *available at* http://www.hosteny.com/funcases/highwayman.html (last visited Aug. 10, 2004).

The romantic side of highwaymen and pursuit of them by law enforcement is captured in Alfred Noyes' famous early twentieth century poem, *The Highwayman*. The landlord's black-eyed daughter, Bess, is ultimately used by the Red-Coat soldiers to snare the highwayman who vows to return to her:

> "One Kiss, my bonny sweetheart, I'm after a prize to-night,
> But I shall be back with the yellow gold before the morning light;
> Yet if they press me sharply, and harry me through the day,
> Then look for me by moonlight,
> Watch for me by moonlight,
> I'll come to thee by moonlight, though hell should br the way."
> ALFRED NOYES, THE HIGHWAYMAN (Stanza V) (Charles Keeping, Oxford University Press, 1983), *available at* http://www.potw.org/archive/potw85.html (last visited Aug. 10, 2004).

[68] Electronic Communications Privacy Act of 1986 § 108(b), 18 U.S.C. § 3117(b) (2001). This definition is broad enough to encompass toll tags, as well as the beepers and GPS devices more frequently used by law enforcement.

[69] S. REP. NO. 99-541, at 10 (1986).

[70] 18 U.S.C. § 2510.

[71] 18 U.S.C. § 3117. These tracking device warrants issued under Federal Rules of Criminal Procedure Rule 41, may provide for use of the tracking devices outside the geographical jurisdiction of the authorizing court.

Beepers

Law enforcement use of beeper[72] transmitters became widespread by the second half of the twentieth century. Attached to a person or object, such as a vehicle, so that the person or object can be followed from a remote location, beepers are simple and relatively inexpensive devices. Usually a beeper takes the form of a battery-operated one-way transmitter that continuously emits an electronic signal that is inaudible at the place from which the signal is transmitted. Beepers are often quite small – usually smaller than toll-tag transponders. They can be attached to a vehicle in a hidden spot, perhaps under a bumper, or placed in a container or even on a person. Miniaturized beepers, about the size of a capsule are sometimes implanted in pets, and even people (such as Alzheimer patients), to help find the persons or pets, should they become lost.

In law enforcement investigations, agents attach a beeper to someone or something they want to track from a remote monitoring post or a patrol vehicle. A receiver operator located away from the target, and unseen by the targeted person follows the electronic signal continuously emitted from the transponder. The direction and distance from which the signal comes, as the signal moves from place to place, is indicated by varying frequencies of beeps heard by the operator. These sounds gave rise to the name, "beeper." Beepers are often used when visual surveillance either does not work or is intermittently lost in following a target. In *United States v. Knotts,*[73] the United States Supreme Court upheld the use of such beepers as an aid to visual surveillance.[74] Later in *United States v. Karo,*[75] the Court limited the use of beepers to areas outside the home.[76] According to the Court's opinion in *Karo*, monitoring a beeper becomes a search under the Fourth Amendment when it reveals "a critical fact about the interior" of a home that could not have been obtained by visual surveillance.[77] As will be discussed in more detail below, when they are followed on the open road, beepers generally do not raise Fourth Amendment issues.[78]

With the enactment of the Electronic Communications Privacy Act in 1986, federal electronic surveillance statutes[79] explicitly recognized the use of beepers and other electronic tracking devices.[80] According to the District of Columbia Court of Appeals in *United States v. Gbemisola,*[81] the sole function of the electronic tracking device section (§ 3117) of the electronic surveillance statute is to authorize monitoring of

---

[72] Beepers are distinguished from bugs because beepers only indicate the location of the signal-emitting transmitter. Beepers do not have the capacity to overhear conversations or intercept communications. "Bugs" and "bugging" normally refer to hidden microphones used to surreptitiously hear and record conversations near the location of the microphone by remote listeners or recorders.

[73] 460 U.S. 276 (1983).

[74] *Id.*

[75] 468 U.S. 705 (1984). *See also* United States v. Application of the United States for an Order Authorizing the Installation, Monitoring, Maintaining, Repairing, & Removing of Elec. Transmitting Devices & Infra-Red Tracking Devices on or Within a White Ford Truck, 155 F.R.D. 401 (D. Mass. 1994).

[76] Karo, 486 U.S. at 715.

[77] *Id.*

[78] *See* text *infra* notes 172-93.

[79] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[80] 18 U.S.C. § 3117 (2001).

[81] 225 F.3d 753 (D.C. Cir. 2000) *cert denied*, 531 U.S. 1026 (2000). *Gbemisola* involved a beeper hidden in an international shipment of heroin hidden in ceramic pots. *Id.* at 755. A vehicle (taxi) was only tangentially involved in the investigation. *See id.* A California Court of Appeal made a similar ruling in a similar beeper case involving importation of heroin that only incidentally involved a vehicle. People v. Salih, 219 Cal. Rptr. 603 (Cal. Ct. App. 1985).

electronic devices, such as beepers, outside the jurisdiction of the authorizing judicial officer. Such beeper warrants were an early example of "roving warrants" which became controversial when the USA PATRIOT Act authorized extension of roving warrants to agencies gathering foreign intelligence.[82]

GPS Devices

Global Positioning System (GPS) devices used by law enforcement agencies are small, but usually larger than beepers. They contain not only a GPS satellite communications function that pinpoints the device's location.[83] They also contain computerized recording devices, or logs. Law enforcement agents attach a GPS device to the underside of a vehicle, in a place where it will not be noticed. From then on the device automatically keeps a detailed time and place itinerary of everywhere the vehicle travels and when and how long it remains at various locations. Later, law enforcement agents remove the device and download the detailed itinerary of where and when the vehicle has traveled. Unlike beepers, GPS devices do not require continuous monitoring by a law enforcement agent.[84]

In a murder case involving a father prosecuted for the murder of his daughter, whose body remained hidden for a substantial period of time, the Washington Supreme Court described police use of a GPS device.[85] The defendant was not informed about the GPS devices that, pursuant to warrants, had been connected to the 12-volt electrical systems of his vehicles while the vehicles were impounded by police. Based on information from the devices, police tracked the vehicles to two locations where evidence of the murder and the body of the victim were eventually found several weeks after the murder. The court explained that, "Use of the GPS devices allowed the vehicles' positions to be precisely tracked when the data from the devices was downloaded."[86] GPS devices facilitate automatic tracking by electronic means, obviating the need for human trackers.

As noted earlier, vehicle owners often voluntarily install GPS devices a part of telematics systems for travel assistance and emergency purposes. If a GPS-equipped vehicle is stolen, the device can be useful in retrieving the vehicle. In a number of successful prosecutions for car theft, stolen vehicles were located through GPS systems voluntarily installed in vehicles by their owners.[87]

Wireless Telecommunications

Wireless Telecommunications and the automatic location information required as part of wireless telecommunications services[88] are also available to law enforcement for tracking purposes. A recent decision

---

[82] USA PATRIOT Act of 2001 § 206, 50 U.S.C. § 1805(c)(2)(B) (2001).

[83] *See* discussion of GPS *supra* notes 50-51.

[84] In a case involving a prosecution for cultivating marijuana in a National Forest, Drug Enforcement agents used both a beeper (a Birddog 300) and a GPS device on a defendant's vehicle. United States v. McIver, 186 F.3d 1119 (9th Cir. 1999).

[85] State v. Jackson, 76 P.3d 217 (Wash. 2003). The facts of this case and the use of GPS monitoring are comparable to similar aspects of the California prosecution of Scott Peterson for the murder of his wife and unborn son. Peterson was tracked from January to April 2003 through a GPS device attached to several of Peterson's vehicles. Information from the devices that showed that Peterson had made repeated trips to the place where the victim's bodies were later found, was admitted at trial. Stacy Finz et al., *Groundbreaking Ruling in Peterson Trial; Tracking Device Evidence Can Be Presented*, SAN FRANCISCO CHRON., Feb. 18, 2004, at A11.

[86] Jackson, 76 P.3d at 257.

[87] *E.g.,* Hicks v. State, 852 So. 2d 954 (Fla. Dist. Ct. App. 2003); State v. Morton, 81 P.3d 461 (Kan. Ct. App. 2003); State v. Bailey, 577 S.E.2d 683 (N.C. Ct. App. 2003). Each of these cases involved use of the GPS aspects of an OnStar telematics system.

[88] See text, *supra* notes 60-61.

upholding law enforcement's tracking of suspects through wireless communications is *United States v. Forest.*[89] The Sixth Circuit approved Drug Enforcement Administration (DEA) agents' controversial surveillance technique that found and followed drug suspects by calling a cellular telephone in the vehicle in which the drug dealers were making their rounds. Since cellular telephones seem to be standard equipment for drug dealers, the DEA agents repeatedly called the cell phone, but hung up before the phone rang. Even without ringing the cell phone, the calls generated "cell-site data" that allowed the agents to find and to follow the suspects, partly through visual surveillance and partly through tracking the cell site data. The Sixth Circuit Court of Appeals ruled that law enforcement use of the cellular telephone site data indicating the suspects's location was not a tracking device, nor did use of the cell-site location data involve interception of communications protected under the federal electronic surveillance laws.[90]

Photo Radar and Photo Red Light

Photo radar and its companion technology, photo red light, are applications of remote camera and license plate recognition systems discussed above. They represent an automated approach to enforcement of traffic laws. Both photo radar and photo red light use digital cameras to automatically generate traffic tickets for speeding and red light running, respectively. These automated traffic tickets usually contain digital pictures of the traffic violation and of the offending driver as he or she appears though the windshield at the time of the violation. These automatic tickets also usually include a digitized picture of the license plate, since license plate recognition is used to connect the vehicle's license plate to the name and address of the vehicle's registered owner. So far, this automated traffic law enforcement does not rely on facial recognition, such as the controversial FaceIt software.[91] But in the future, such automated facial recognition technology may be added, if it is found to be sufficiently accurate in this context.

Red light cameras and photo radar are often combined into a system of automatic traffic enforcement.[92] The automatic surveillance cameras can be either autonomous units at fixed sites, or under the control of an officer in a patrol car. The digital cameras may be hidden, or may be visible and even accompanied by warning signs that photo radar or photo red light technologies are in use. The units are programmed to capture images only when a traffic violation, such as running a red light or speeding, occurs. Triggered by such a violation, the camera automatically records the violation and its perpetrator and then sends the digital information to a processing center for the automatic generation of a traffic citation. The citation may even be automatically addressed and mailed to the registered owner of the vehicle, who is presumed to be the perpetrator. The entire traffic enforcement process is almost untouched by human hands.

When red light and photo radar cameras are located at highly visible fixed sites or are accompanied by signs giving notice of the cameras' presence, they are used to deter traffic infractions by emphasizing the likelihood of being caught. High visibility cameras are often used to discourage speeding in school zones or running red lights at particularly dangerous intersections where fatalities have occurred in the past. A typical high-visibility deterrence technique combines a portable photo radar unit with a variable message sign that informs drivers about just how fast they are driving in a restricted speed zone. As might be expected, several states have outlawed the use of photo radar as unfair, or as "just not sporting" as some photo radar opponents often put it.

---

[89] 355 F.3d 942 (6th Cir. 2004).

[90] *But see*, Company v. United States (In re United States), 349 F.3d 1132 (9th Cir. 2003). The Ninth Circuit did not reach the electronic surveillance issues. *Id.* Instead, the Ninth Circuit Court of Appeals held that requested law enforcement use of a telematics communication system for the purpose of intercepting communications taking place in the telematics-equipped car was improper because it interfered with the emergency response features of the telematics communication system. *Id.*

[91] FaceIt software, Identix, Inc. website, *at* http://www.identix.com/products/pro_sdks_multi.html (last visited Aug. 10, 2004).

[92] A typical combined system of this type is illustrated at the Redflex Holding Limited website, *at* http://www.redflex.com (last visited Aug. 10, 2004).

These are just some of the broad array of technologies available to intelligence agencies and law enforcement for use in finding and tracking people on the open road. From electronic tracking devices, such as beepers and GPS devices, to cell phones and even photo radar, law enforcement is well-equipped technologically to track people on the open road. Law enforcement agents are likely also to be allowed to access information from non-law enforcement systems, such as information generated by toll tags and other aspects of ITS. In fact, the USA PATRIOT Act was designed to provide law enforcement more ready access to just such records.[93]

III. Privacy Interests on the Open Road

Since where a person is located reflects who that person is, individuals are concerned when somebody else scrutinizes their whereabouts. Individual privacy is affected when others keep track of a person as she or he moves about in physical space on public roads. A person's location and travel patterns reveal the person's activities, associations and what he or she considers important. The technologies discussed in the previous section can follow an individual's every movement on public roadways in real time on a continuous basis. Often this scrutiny is unseen by the individual. But the possibility of scrutiny is omnipresent. As a result, individuals have no way of knowing whether or when their activities are being watched.

Logically, activities that are open to sight and hearing, such as traveling on a public road, do not seem to be very private. And yet even out on the open road certain privacy interests remain significant. Understanding the privacy interests affected when a person's on-the-road activities are, or can be, tracked and recorded requires looking beyond what appears to be a surface contradiction between privacy and the open road.

The moral philosopher, Jeffrey Reiman examined the privacy interests of people traveling along public roadways in his seminal *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future.*[94] The article suggests the image of a panopticon (literally an all-seeing device) which Jeremy Bentham advocated as a powerful prison design in 1791. Bentham's concept of a panopticon prison made each prisoner's every movement continuously visible to guards who could watch all of the prisoners all of the time. Bentham noted that in practice it would not be necessary to have guards actually watch each prisoner at every moment. Simply the potential for complete and continuous visibility would cause each prisoner to watch himself all the time. Such a system would, Bentham argued, give the state even more power over prisoners than keeping the prisoners bound in chains. In short, the panopticon was designed to give authorities intense control over prisoners.[95] Concerns about abject conformity and warped human personalities that could result from such a dystopian everyone-is-visible-all-the-time regime was, of course, part of the searing image of an all-seeing Big Brother in George Orwell's novel, 1984.[96] The world of the panopticon, or of 1984, offers a powerful perspective on some of the privacy interests at stake on the open road.

Defining privacy as "the condition in which others are deprived of access to you,"[97] Reiman describes some of the moral risks posed by a complex of information-gathering and surveillance focused on highway travelers. One such risk is the vulnerability of people, whose movements are monitored, to having their behavior controlled by others through pressures, legal and otherwise, for social conformity, rather than through independent thought and action. Moreover, Reiman warns against the destructive effect on human personality

---

[93] USA PATRIOT Act of 2001 § 206, 50 U.S.C. § 1861 *et seq.* (2001).

[94] Jeffrey H. Reiman, *Driving to the Panopticon: A philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L. J. 27 (1995).

[95] Michel Foucault emphasized this point in his discussions of what Foucault called "panopticism." MICHEL FOUCAULT, DISCIPLINE AND PUNISH 195-228 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1978).

[96] ORWELL, *supra* note 7.

[97] Reiman, *supra* note 94, at 30.

of not having control over who observes and keeps track of an observed individual.[98] Indeed, comprehensive surveillance tends to be socially destructive because it signals disrespect for the individual person by treating her as an object, rather than as a self-determining individual. In the end, pervasive surveillance can distort the very nature of a human personality. It saps a person of dignity and self-respect by distorting the way the individual thinks of himself and for himself. The individual person becomes an object to be acted upon, rather than a morally responsible actor.

Privacy interests are grounded in such concerns about individual worth and self-determination,[99] the right of an individual to decide for herself where she will go and what she will do. Although writers about privacy have long argued about particular language or categories describing privacy,[100] modern legal analysis conventionally divides privacy interests into two categories: autonomy privacy (or decisional privacy) interests and information privacy (or data privacy) interests.[101] Privacy interests in the context of public roads and highways are notable in combining both autonomy privacy interests and information privacy interests, as well as a third factor that affects both categories of privacy interests. This third factor is the panopticon effect of comprehensive surveillance suggested by Professor Reiman, as discussed above.

Autonomy Privacy Interests

Autonomy privacy interests are characterized by a person's ability to make decisions and to act "without observation, intrusion or interference."[102] Indeed, surveillance of people on the open road implicates several types of autonomy interests, such as the right to go where one wants to go without being watched, the right to consent, or not, to others' use of one's travel patterns, and the right not to be intruded on by oppressive governmental or private-sector entities - Big Brother, Big Sister and the gang of little brothers noted at the beginning of this article. Although, autonomy privacy is often associated with intimate choices such as those regarding sex and procreation, other much less intimate choices and activities also deserve protection against outside interference.

Protection of autonomy has historically embraced freedom of movement. For example, Justice William O. Douglas, in describing various zones of privacy, envisioned an outermost privacy zone where the individual has "freedom to walk, stroll, or loaf."[103] Surveillance systems, such as those described above, whether they are law enforcement or ITS systems, affect the autonomy of travelers by overriding individual control over who or what watches and keeps track of an individual's movements from place to place. Travelers forced look over their shoulders for surveillance systems are affected by not knowing whether or when their actions are being captured by others. Particularly in choices about whether or not to do something unconventional or to go to a

---

[98] Jeffrey Rosen has made a similar point in his books. *See* JEFFREY ROSEN, THE NAKED SOCIETY (2003); JEFFREY ROSEN, THE UNWANTED GAZE (2000).

[99] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890). Brandeis, who was the primary author of the article referred to privacy as the individual's right to an "inviolate personality." *Id.* at 205. *See* Dorothy Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1 (1979).

[100] For leading legal theoreticians who propose different views of privacy see ARTHUR R. MILLER, THE ASSAULT ON PRIVACY (1971); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964); Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968); Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

[101] This 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 (1879)). Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 654 (Cal. 1994). The court described information privacy as "interests in precluding the dissemination or misuse of sensitive and confidential information." *Id.* Autonomy privacy refers to "interests in making intimate personal decisions or conducting personal activities without observation, intrusion or interference." *Id.*

[102] *Id.*

[103] Doe v. Bolton, 410 U.S. 179, 213 (1973) (Douglas, J., concurring).

potentially controversial place, this uncertainty can be stifling. When such surveillance is under the control of the government, privacy concerns become also political concerns about centralizing too much power in a overbearing state.

Roadway surveillance affects autonomy privacy interests in several ways. First, unseen collection of information about where people travel is often connected up with these travelers' personal data, consumption patterns or other information about them, without the persons involved being aware of, much less consenting to the collection of the information. When such information is combined and consolidated with other personal information into a profile of an individual's supposed personal characteristics, the individual deserves to be consulted. Even aside from information privacy issues discussed below, such practices treat people as objects, rather than as autonomous persons. Such practices also make people fear potential consequences such as increased insurance rates, marital discord, or the appearance of hypocrisy. Even when marketing companies do not identify particular drivers, individuals whose movements are monitored without their consent often feel manipulated by being turned into fodder for an unseen data base in which the individuals did not agree to participate.

Moreover, people feel violated when surveillance results in feedback in the form of marketing pitches based on "personal" profiles used to label them as belonging in one consumer category or another. For example, people who regularly travel between particular geographic areas may be "branded" as having particular characteristics, such as income level or ethnicity. Although demographic information in such profiles may be aggregated, the potential for disaggregation, to the point of identifying a particular person, causes further privacy concerns. After all, when aggregate data is"sliced and diced" (as the marketing industry aptly describes techniques of data analysis), it often becomes possible to narrow the reference down to a particular individual. For example, sorting by zip code, then year and type of vehicle, and perhaps age can sharpen the demographic focus to just one or two people.

In addition, advertising use of demographic information often seeks to psychologically manipulate consumers targeted according to the neighborhood in which they live or the locations to which they travel. Most people find receiving unsolicited information from an anonymous source that knows where they live, where they have driven recently and where they regularly travel to be very unsettling and intrusive. In the future, when drivers receive such targeted information from their on-board DSRC unit as they drive from one place to another, the sense of intrusion, not to mention the noise level, is likely to be magnified. In the near future, telematics systems will automatically beam billboard-type advertising into vehicles by sending location-based advertising messages directly targeted to identified drivers. When that happens complaints about intrusion are likely to rise. Drivers intruded upon by such targeted marketing messages may find this beamed advertising much more intrusive than billboards, which drivers can simply refuse to look at.

Finally, an individual may never know that law enforcement agencies, perhaps for intelligence or investigative purposes, not only have collected surveillance information but also have gained access to privately collected consumer data. Even law-abiding drivers may feel the pressure of such potential unseen government scrutiny. As law enforcement concerns about terrorist threats involving transportation systems has increased, people are aware of an increased emphasis on watching out for threats and dangerous people on the nation's often-congested highways. Most people on highways probably share such concerns about homeland security. But they also may find that their autonomy is constrained by the potential for being watched and recorded everywhere they go on what still ironically called "the open road."

Information Privacy Interests

Information privacy interests are concerned with "precluding the dissemination or misuse of sensitive and confidential information."[104] Information privacy interests are affected when surveillance systems collect, categorize, use and store information about a person's whereabouts, both past and present. When that is done without the person's consent, the autonomy privacy interests discussed above are also affected. Because a

---

[104] Hill, 865 P.2d at 654.

person's location at a particular moment may also be very sensitive information, such roadway surveillance often affects information privacy interests as well. Personal location information, for example, may be just what an individual does not want others, such as a stalker, to know. Although a person's pattern of travel is rarely completely secret or confidential, a person expects that her movements from place to place will be evanescent, leaving no permanent trace.

Alexander Sholzenitzen captured the sense of being trapped by records in his famous image of personal information as the strands of a spider web:

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence. . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.[105]

Information about a person's movements in physical space belongs, in a fundamental sense, to the person without whom such information could not exist, whose travel decisions created the pattern of information and whose very personality is embodied in the pattern. An anonymous surveillance system or transportation database that captures those patterns, lacks the originating individual's claim to ownership.

Surveillance systems that collect and digitize information about a person's present and past locations and travel patterns are making use of information that properly belongs to the individual traveler. Use by others of personal information about an individual without the individual's consent interferes with the individual's information privacy interests. These information privacy interests include both consenting or refusing to consent to collection of information about one's location and travel, as well as preventing dissemination or misuse of personal details about one's life and travels. Dossiers, itineraries, profiles of the places where a person has been, all impinge on important information privacy interests of an individual. When the individual who is the subject of the information has no way of knowing about or affecting the collection of the information by unseen surveillance systems, the individual is powerless to affect, much less constrain, use of the individual's personal information by invisible users.

Information collected through roadway surveillance can be used to annoy the individual through targeted marketing and advertizing. Such information can also be used to harass the individual through stopping and questioning her. Such information may even be used by stalkers to frighten or even to kill the individual. Such information can be used by government agencies, including law enforcement and intelligence agencies, to find suspicious individuals for detention or control. Roadway surveillance information can also be used to profile individuals, to predict their future actions, and to psychologically manipulate their choices about where to travel.

The ITS technologies discussed above have a particularly high potential for affecting information privacy. License plate recognition systems can note the location of a particular vehicle and keep track of other locations where that vehicle has appeared over time. Prediction of a person's future movements can be based on profiles compiled from past archived itineraries. Remote traffic cameras that capture digital images of individuals and vehicles can locate a person, whether she is a driver or a passenger or even a pedestrian or passerby. These digital images can be stored indefinitely for future reference. Beepers and toll tag transponders can also be used follow the movements of a person and pinpoint that person's current location. GPS devices secreted on a vehicle can keep detailed logs of the times and places of all movements for later downloading and

---

[105] ALEXANDER I. SOLZHENITSYN, CANCER WARD (1968).

analysis. Cellular telephone technology's required automatic location information provides real-time information about the location of a wireless telecommunication device and its user's movements from place to place. Archives of individual itineraries derived from all of these technologies can be used both to associate an individual with locations the individual frequented in the past, as well as to predict future destinations.

Whenever information about an identified or identifiable person is collected, information privacy interests are affected. In some ways, ITS applications can be more mindful of these informational privacy interests than other types of surveillance because ITS has the advantage of being an application of intelligent systems. The intelligence of these systems is useful not only in solving transportation problems, but also in building privacy protections into the very architecture of the technologies. For example, an intelligent system can be designed so that it does not collect information about individuals at all. Alternatively, an intelligent system can be designed to minimize the personal information that is collected and how long the information is kept, as well as to restrict the availability of the information to others. When intelligent systems collect individually identifiable information, that information can be automatically encrypted using strong encryption and automatically destroyed when a transitory purpose, such as ascertaining real-time traffic speed, is past. Indeed, responsible ITS agencies have required that privacy protection be built into ITS systems which may affect information privacy interests.[106]

Other not-so-intelligent attempts to do something about privacy will not work very well. For example, developers of ITS systems designed to collect and distribute large amounts of personally identifiable information may just add on privacy protection at the last stage of the design, rather than building privacy into way the ITS system is organized. When such information privacy add-ons are pasted onto a surveillance system that maximizes collection and exposure of personal information, it is quite easy for hackers or intelligence agencies to circumvent such measures by simply going upstream in the data flow - after the data is collected but before the privacy protections apply. For example, a traffic surveillance system that uses license plate recognition to time vehicles at successive locations to determine traffic speed may eventually encrypt the digitized license plate information. However, someone else, say a private investigator or an intelligence agency, can either routinely or in particular cases reach in and capture the data before it is encrypted. Unauthorized persons, whether a private investigator working a domestic relations case or a stalker bent on mayhem, may also capture information about particular vehicles associated with targeted people, through such an "upstream" access. The result is unintelligent and ineffective privacy protection.

Fortunately, responsible members of the ITS industry, with assistance from the Intelligent Transportation Society of America (ITS-America) the trade association of the ITS industry, have adopted privacy principles that recognize the need to protect information privacy as part of ITS intelligent systems. These principles urge development of ITS applications that are designed to protect information privacy from the ground up. ITS America's "Intelligent Transportation Systems Fair Information and Privacy Principles" were "prepared in recognition of the importance of upholding individual privacy in implementing Intelligent Transportation Systems (ITS). . . . Initiators of ITS projects are urged to publish the fair information and privacy principles that they intend to follow. Parties to ITS are urged to include enforceable provisions for safeguarding privacy in their contracts and agreements."[107] These principles are not perfect protections for

---

[106] For example, the TravInfo traveler information system in the San Francisco Bay area has embraced significant privacy protections. *See* 511 Traffic website, *at* http://traffic.511.org/privacy.asp (last visited Aug. 10, 2004). *See also* Adam Clymer, *Tracking Bay Area Traffic Creates Concern for Privacy,* N.Y. TIMES, Aug. 26, 2002, at A11.

[107] S*ee* Fair Information and Privacy Principles, Intelligent Transportation Society of America (ITS) website, *at* http://64.233.167.104/search?q=cache:1Epp7uNV2GoJ:www.itsa.org/subject.nsf/836e8941046dcc0e852565860062db0d/c34171cc9664b456852569430060955a/%24FILE/Board%2520Approved%2520Privacy%2520Principles.doc+%22prepared+in+recognition+of+the+importance+of+upholding+individual%22&hl=en (last visited Aug. 10, 2004). The ITS-America information privacy principles include the following:

1. INDIVIDUAL CENTERED. Intelligent Transportation Systems must recognize and respect the individual's interests in privacy and information use.

2. VISIBLE. Intelligent Transportation Information Systems will be built in a manner "visible" to individuals.

3. COMPLY. Intelligent Transportation Systems will comply with applicable state and federal laws governing privacy and information

information privacy. But they do recognize the need to respect the information privacy interests of individuals whose lives may be caught up in ITS systems.

The Panopticon Effect

The collection of personal information by impersonal government and private-sector roadway surveillance agencies also has political, as well as psychological and practical dimensions. Authoritarian systems can misuse information about individuals to round up suspects or to treat people as undesirables based on where they are or have been. Systems that comprehensively keep track of the whereabouts of each person in all places and at all times produce profiles or predictive patterns of where a tracked person is likely to be found and where that person is likely to go. The destructive psychological effect of maintaining centralized information about each individual compromises these individuals' self-determination and autonomy. As noted above, a person who knows that she is, or can be, constantly watched is not free. In addition, comprehensive centralized tracking systems can also use that information to affect the individual's future choices about where it is "safe" or "not safe" to go. Human nature tends to resist being categorized, manipulated psychologically, intimidated and mechanistically predicted by society. But with comprehensive surveillance in place, every time a person goes from one place to another on public roads, the surveillance would both take its toll on the individual and also concentrate great power in those in control of the surveillance. This combination of factors impinging on individual freedom is the panopticon effect.

The panopticon effect is a predictable result of wide-scale comprehensive surveillance. Indeed, Michel Foucault described "panopticism" as a key mechanism of centralized social control.[108] The combination of technologies described in the previous part of this article have the capacity to create a world in which the panopticon is a reality for those who travel on public roadways. The pervasiveness of modern roadway surveillance technologies makes it possible for a central authority to find, to follow and to keep track of nearly everyone. Almost any individual's movements from place to place can be tracked without the individual knowing whether or not she is being tracked, or has been tracked. The realization that such centralized tracking is possible impresses a profound sense of powerlessness upon an individual and affects her choices about where, and where not, to go. That is the panopticon effect. For those concerned about individual privacy, centralized systematic scrutiny that is ubiquitous as well as covert simply represents too much societal control over the individual. It makes ordinary drivers feel as if they were prisoners in Jeremy Bentham's prison, rather than presumptively law-abiding people on the open road. With roadway surveillance technologies multiplying into so many avenues of societal control, there appear to be few escape routes for individual freedom and imagination. The panopticon will have become a reality when individual choices about where to go and what to do are under the control of the system.

A century and a half ago, in writing about the Constitutional History of England, Sir Thomas May noted the problematic consequences of the panopticon effect:

---

use.

4. SECURE. Intelligent Transportation Systems will be secure.

5. LAW ENFORCEMENT. Intelligent Transportation Systems have an appropriate role in enhancing travelers' safety and security interests, but absent consent, statutory authority, appropriate legal process, or emergency circumstances as defined by law, information identifying individuals will not be disclosed to law enforcement.

6. RELEVANT. Intelligent Transportation Systems will only collect personal information that is relevant for ITS purposes.

7. ANONYMITY. Where practicable, individuals should have the ability to utilize Intelligent Transportation Systems on an anonymous basis.

8. COMMERCIAL OR OTHER SECONDARY USE. Intelligent Transportation Systems information stripped of personal identifiers may be used for non-ITS applications.

9. FOIA. Federal and State Freedom of Information Act (FOIA) obligations require disclosure of information from government maintained databases. Database arrangements should balance the individual's interest in privacy and the public's right to know.

10. OVERSIGHT. Jurisdictions and companies deploying and operating Intelligent Transportation Systems should have an oversight mechanism to ensure that such deployment and operation complies with their Fair Information and Privacy Principles. *Id.*

[108] *See* FOUCAULT, *supra* note 95, at 195-228.

> Next in importance to personal freedom is immunity from suspicions and jealous observation. Men may be without restraints upon their liberty; they may pass to and fro at pleasure; but if their steps are tracked by spies and informers, their words noted down for crimination, their associates watched as conspirators, - who shall say that they are free? Nothing is more revolting . . . than the espionage which forms part of the administrative system of continental despotisms. It haunts men like an evil genius, chills their gayety, restrains their wit, casts a shadow over their friendships, and blights their domestic hearth. The freedom of a country may be measured by its immunity from this baleful agency.[109]

Modern courts in the United States sometimes sound similar alarms.

In an Oregon decision involving a beeper attached without a warrant to a burglary suspect's automobile, the Oregon Supreme Court expounded his state's constitutional right to freedom from technologically advanced scrutiny:

> Since 1859 . . . [when the Oregon Constitutional provision was adopted], the government's ability to scrutinize the affairs of "the people" has been enhanced by technological and organizational developments that could not have been foreseen then. Tiny radio transmitters for surreptitiously locating objects to which the transmitters are attached are among these developments. . . . Any device that enables the police quickly to locate a person or object anywhere within a 40-mile radius, day or night, over a period of several days, is a significant limitation on freedom from scrutiny. . . . The limitation is made more substantial by the fact that the radio transmitter is much more difficult to detect than would-be observers who must rely upon the sense of sight. Without an ongoing, meticulous examination of one's possessions, one can never be sure that one's location is not being monitored by means of a radio transmitter. Thus, individuals must more readily assume that they are the objects of government scrutiny. . . . [F]reedom may be impaired as much, if not more so, by the threat of scrutiny as by the fact of scrutiny. . . . [If no warrant is necessary for the use of an electronic transmitter], no movement, no location and no conversation in a "public place" would in any measure be secure from the prying of the government. There would in addition be no ready means for individuals to ascertain when they were being scrutinized and when they were not. That is nothing short of a staggering limitation upon personal freedom.[110]

When the Oregon court warned about infringing the right to be free from scrutiny, it was calling for opposition to the panopticon effect.

In the State of Washington, the supreme court raised similar concerns about the panopticon effect in a case involving use of GPS devices. The Supreme Court of Washington upheld the use of the GPS devices because the devices' installation and use were authorized by judicial warrants. In discussing the importance of requiring warrants in cases involving such surveillance technologies, the court warned:

> [T]he intrusion into private affairs made possible with a GPS device is quite extensive as the information obtained can disclose a great deal about an individual's life. For example, the device can provide a detailed record of travel to doctors' offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise gyms, places where children are dropped off for school, play, or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball game, the "wrong" side of town,

---

[109] THOMAS E. MAY, 2 CONSTITUTIONAL HISTORY OF ENGLAND SINCE THE ACCESSION OF GEORGE THE THIRD 1760-1860 275 (Boston: Crosby & Nichols, 1862-1864), *available at* http://www.don-aitken.freeuk.com/emay3v039.html (last visited Aug. 10, 2004).

[110] State v. Campbell, 759 P.2d 1040, 1048-1049 (Or. 1988)

> the family planning clinic, the labor rally. In this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and foibles. The GPS tracking devices record all of these travels, and thus can provide a detailed picture of one's life. . . .
>
> . . . .
>
> . . . [U]se of GPS tracking devices is a particularly intrusive method of surveillance, making it possible to acquire an enormous amount of personal information about the citizen under circumstances where the individual is unaware that every single vehicle trip taken and the duration of every single stop may be recorded by the government.
>
> We conclude that the citizens of this State have a right to be free from the type of governmental intrusion that occurs when a GPS device is attached to a citizen's vehicle, regardless of reduced privacy expectations due to advances in technology.[111]

The Washington Supreme Court appears to share the Oregon court's call for resistance to the panopticon effect.

The panopticon effect has been a longstanding concern of those interested in promoting technological progress and security. Advocates of technology, as well as privacy advocates, share concerns about the impact of such technologies on human personality and privacy. Technology advocates are worried that the panopticon effect will erode trust in and generate restrictions on roadway surveillance technologies. On the other hand, privacy advocates are concerned about controlling surveillance technologies so that they do not have undesirable personal or political consequences.

More than thirty years ago in *United States v. White,*[112] a plurality of the United States Supreme Court upheld the use of wired informers as not a search or seizure. But two of the dissenting Justices warned about the consequences of not paying attention to the panopticon effect. Justice Harlan, dissenting, insisted on the need for "assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the . . . technique of law enforcement."[113] In his dissenting opinion in *White*, Justice Harlan felt that the law enforcement technology involved in that case had too great an impact on the individual's sense of security. In his dissenting opinion in *White,* Justice Douglas more dramatically warned about the tyranny of technology over humanity. Justice Douglas admonished, "Today no one perhaps notices because only a small, obscure criminal is the victim. But every person is the victim, for the technology we exalt today is everyman's master."[114]

It is important to carefully consider privacy interests before deploying roadway surveillance technologies that can compromise individual privacy and result in a panopticon effect. Indeed, there is a history of adverse public response to government programs designed to collect information about individuals. When these surveillance systems appear to be building blocks toward the construction of a surveillance panopticon, public and political outrage is likely.[115] It is important for those who believe that technology is not incompatible with

---

[111] State v. Jackson, 76 P.3d 217, 223-24 (Wash. 2003).

[112] 401 U.S. 745 (1971).

[113] *Id.* at 786 (Harlan, J., dissenting).

[114] *Id.* at 757 (Douglas, J., dissenting).

[115] For example, negative public response doomed the Department of Defense's infamous "Total Information Awareness"office, even as it was later reconstituted as the "Terrorism Information Awareness" program. *See* discussion *supra* notes 9-11.

Other similar data collection projects are the Justice Department's Matrix (Multistate Antiterrorism Information Exchange) program and the Transportation Security Agency's CAPPS II. With regard to Matrix, see Black, *supra* note 10. Apparently only Florida, Michigan, Connecticut, Pennsylvania, and Ohio continue to cooperate with the program. Schwartz, *supra* note 10. With regard to CAPPS II, an updated version of the existing airport screening program, Computer-Assisted Passenger Prescreening System, see Behar, *supra* note 11. Concerns about the privacy of screening information has caused repeated delays in the launch of CAPPS II.

privacy to assure that the many new forms of roadway surveillance do not loom over the nation's highways like a panopticon.

IV. Legal Protection for Privacy on the Open Road

Courts and legislatures across the United States are keenly aware of the privacy interests discussed in the previous part of this article. Balancing what is properly protected as private against what needs to be public in a roadway setting is often difficult. As a result, decision makers usually recognize that roadway privacy protections are virtually never absolute, but rather depend on particular circumstances. As courts and legislatures balance both individual and societal concerns in determining whether a particular type of roadway surveillance requires restriction for privacy reasons, they often focus on larger societal implications, such as the panopticon effect. When roadway surveillance appears to result in overwhelming societal control over individuals, privacy interests are most likely to prevail in both public policy and legal determinations.

In many cases, the balance between what is appropriately private and what is necessarily public on the road is expressed in terms of reasonable expectations of privacy, a concept that will be examined first. Then Fourth Amendment restrictions on stopping vehicles on roadways will be contrasted with Fourth Amendment tolerance of tracking people on roads and highways. After considering some of the cases imposing tort liability for interfering with the privacy of people on roadways, this discussion of legal protections for privacy on the open road will conclude with a look at some specific statutes enacted to protect roadway privacy against surveillance technologies.

Reasonable Expectations of Privacy on the Open Road

Legal protections for privacy, both on the open road and elsewhere, are often described in terms of reasonable expectations of privacy. "Reasonable expectations of privacy" usually expresses a conclusion that an individual's privacy interests outweigh the interests of society. Although most commonly used in deciding whether there has been a violation of the Fourth Amendment's prohibition against unreasonable searches and seizures, the reasonable expectations of privacy concept also appears more broadly in other types of privacy laws, including tort, state constitutional protections and even privacy legislation. Whether reasonable expectation of privacy analysis is useful in considering privacy protections on roads and highways is a deeper question about which there is substantial disagreement.

Analysis of privacy cases in terms of "reasonable expectations of privacy" is based on Justice Harlan's concurring opinion in *Katz v. United States*, a case involving privacy claims that surreptitiously recorded conversations from a public phone booth should be suppressed. The majority opinion by Justice Stewart rejected earlier interpretations of the Fourth Amendment that limited its protections to instances where government agents had trespassed on property interests of the person claiming Fourth Amendment protection. In ruling that the Fourth Amendment "protects people, not places,"[116] Justice Stewart, writing for the majority, rejected the older property-based limitations that had routinely withheld Fourth Amendment protections from people in public places, such as roads and highways.

Justice Harlan's concurring opinion in *Katz* added that decisions whether or not the Fourth Amendment's probable cause and warrant requirements should apply at all require consideration of two separate issues: "My understanding of the rule that has emerged from prior decisions is that there is 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.'"[117] Although Justice Harlan continued to believe that the place where a person is located is relevant in such an analysis, he insisted that even in public places there are areas where "occupants' expectations of freedom from intrusion are recognized as

---

See, e.g., Verton, *supra* note 11; Wald, *supra* note 11.

[116] Katz v. United States, 389 U.S. 347, 351 (1967). Although Katz was in a public place, the Court insisted that "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.*

[117] *Id.* at 361 (Harlan, J., concurring).

reasonable."[118] Over the years Justice Harlan's two-fold reasonable expectation of privacy analysis morphed from an inquiry whether an expectation of privacy was subjectively and objectively "reasonable"[119] into similar inquiries into whether such the privacy expectation was "justifiable"[120] or "legitimate"[121] or sometimes all three.[122]

Reasonable expectations of privacy analysis does not work very well in considering privacy interests in public roadway contexts. A person on a road seems, almost by definition, to lack both the subjective and objective elements of a reasonable expectation of privacy. And yet, there are numerous instances where the privacy of people on public roads has been protected by law. Protecting privacy on public roadways is a feature of search and seizure decisions as well as of applications of state constitutional privacy guarantees. Damage actions for intrusion on the privacy of people on roads and highways are also possible. Moreover, such privacy claims are reflected in legislation designed to rein in surveillance technologies used on public roadways. It is possible to construe these legal privacy protections for privacy on the open road as just reflections of subjectively and objectively reasonable expectations of privacy. But such a reasonable expectations of privacy analysis does not reach the deeper questions of whether and when privacy ought to be protected in this setting.

When the privacy of people on public roads is legally protected, two types of factors are usually important: context factors and consequence factors. First, the context in which the issue of protecting privacy is raised is important. In court cases, the procedural context is also significant. For example, whether privacy protection is at issue with regard to suppression of a particular item of evidence in a criminal prosecution is a different procedural context from deciding whether stopping people on highways should be a routine law enforcement practice. Protecting privacy is more likely in the latter type of context. For both courts and legislatures, the factual context, such as how a particular type of surveillance works, and whether surveillance is covert or visible, are also important factors.

Second, the consequences of protecting or not protecting individual privacy in terms of government or private-sector power over an individual are likely to partly determine when the privacy of people on roads and highways should be protected. Ultimately, the overriding issue in these roadway situations focuses on how much societal power over individuals is tolerable. A certain degree of societal control is to be expected, because the open road is a setting where individuals and society interact. But too much societal control stifles individual freedom. Finding an appropriate balance is crucial. Somehow mechanically applying reasonable expectations of privacy analysis seems to obscure this vital point.

Critics of reasonable expectations of privacy analysis come from many different directions. Not all reasonable expectations of privacy critics favor protecting privacy of people on open roads. Perhaps the most acerbic of such critics is Justice Scalia, who complains that the "reasonable expectation of privacy" test lacks any "plausible foundation in the text of the Fourth Amendment," and is also "self-indulgent."[123] He scoffs that, "[U]nsurprisingly, 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

---

[118] *Id.* (Harlan, J., concurring).

[119] Kyllo v. United States, 533 U.S. 27 (2001); *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

[120] "Justifiable" was the chosen privacy-expectation modifier in the plurality opinion in United States v. White, 401 U.S. 745 (1971), which also used "reasonable" and "legitimate" as adjectives. *See also* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 616 (1989).

[121] Couch v. United States, 409 U.S. 322, 336 (1973) (discussing the legitimacy of privacy expectations). *See also* Bartnicki v. Vopper, 532 U.S. 514, 540 (2001).

[122] United States v. Dunn, 480 U.S. 294, 315 (1987).

[123] Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

reasonable."[124]

Even Justice Harlan, who originated reasonable expectations of privacy analysis, later became concerned about its meaningfulness. Four years after concurring in *Katz*, Justice Harlan dissented in *White*, a case in which the United States Supreme Court held that the use of a surreptitiously wired informer did not infringe any reasonable expectation of privacy:

> While ["reasonable expectation of privacy"] [ ] formulations represent an advance over the unsophisticated trespass analysis of the common law, they too have their limitations and can, ultimately, lead to the substitution of words for analysis. The analysis must, in my view, transcend the search for subjective expectations or legal attribution of assumptions of risk. Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present.
>
> Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement.[125]

Undesirable consequences in terms of too much government control over individuals seemed to Justice Harlan to be more important than whether or not people expect that those with whom they talk may be wired informers. For Justice Harlan the real issue was whether or not wired informers were to become an acceptable feature of life in the United States. Justice Harlan thought they should not. That is why he dissented in *White.*

More recently, Justice O'Connor in her majority opinion for the Court in *Indianapolis v. Edmond,*[126] a case involving drug-interdiction roadblocks, discussed below, also reflected a similar uneasiness with reasonable expectations of privacy analysis. In fact she avoided even mentioning reasonable expectations of privacy in ruling:

> Without drawing the line at roadblocks designed primarily to serve the general interest in crime control, the Fourth Amendment would do little to prevent such intrusions from becoming a routine part of American Life . . . .
>
> . . . .
>
> . . . We cannot sanction stops justified only by the generalized and ever-present possibility that interrogation and inspection may reveal that any given motorist has committed some crime.[127]

For Justice O'Connor, the issue was not whether Edmond's expectation of privacy on the highway outside Indianapolis was or was not reasonable. Rather, the issue for Justice O'Connor was the consequences, in particular the type of society fostered by tolerating such a practice of law enforcement routinely stopping law-abiding motorists on the chance that such motorists might be engaged in wrongdoing. She was particularly concerned about preventing the development of a society in which people on roads are forced to assume that they will be routinely stopped by law enforcement without any reasonable suspicion of wrong-doing.

Other jurists have also criticized application of reasonable expectations of privacy analysis to on-the-road contexts from a different perspective. For example, in a series of decisions, the Oregon Supreme Court expressed doubts about "reasonable expectations of privacy" analysis in interpreting state constitutional

---

[124] *Id.* (Scalia, J., concurring) (quoting in part Katz, 389 U.S. at 361).

[125] White, 401 U.S. at 786 (Harlan, J., dissenting).

[126] 531 U.S. 32 (2000).

[127] Edmond, 531 U.S. at 43-44.

protections against illegal searches.[128] In one of these decisions, involving warrantless use of a beeper, Justice Lent bluntly held:

> Because the ["reasonable expectations of privacy"] phrase continues to appear so often in arguments, we hereby expressly reject it for defining searches under [the Oregon Constitution's provisions regarding searches and seizures]. . . . The phrase becomes a formula for expressing a conclusion rather than a starting point for analysis, masking the various substantive considerations that are the real bases on which Fourth Amendment Searches are defined. . . . [The privacy protected by the Oregon Constitution] is not the privacy that one reasonably *expects* but the privacy to which one has a *right*.[129]

Having banished expectations of privacy analysis, the court determined that the Oregon Constitutional right to privacy is violated when police install a tracking device on a vehicle without a warrant.

These judicial opinions, as well as numerous statutes enacted to protect roadway privacy, seek to redirect attention to the societal consequences of protecting the privacy interests of people on the open road. Rather than quibbling about whether such expectations of privacy are subjectively and/or objectively reasonable, these opinions confront the basic issue whether a privacy interest deserves protection in the particular context of roads and highways. Their focus is on assessing the extent to which social control over individuals - whether from Big Brother, Big Sister, the gang of little brothers or some combination of them - is tolerable.

Stopping a Vehicle on the Open Road is a Seizure

Concerns about contexts and consequences of privacy claims, rather than whether expectations of privacy are reasonable, are clearly reflected in recent United States Supreme Court decisions holding that stopping a vehicle on a road or highway is a seizure for the purposes of the Fourth Amendment.[130] In two recent decisions,[131] the United States Supreme Court has required that when law enforcement agents stop vehicles on roadways, these agents must have very good reasons for doing so. As a theoretical matter, there remains an underlying question whether such vehicle stops should occur only in exceptional cases (currently the view of the majority of the Court) or whether vehicle stops should be acceptable as a general rule (currently the view of a minority of the Justices). Insistence that government power over individuals needs to be limited and assiduously prevented from overwhelming individual freedom is part of the underlying explanation for the majority's insistence on protecting privacy on the open road from too many law enforcement stops, roadblocks, checkpoints, and the like.

Law enforcement interest in roadways goes back many centuries.[132] Modern efforts to capture criminal suspects on public roadways intensified early in the twentieth century, with the advent of the automobile and paved highways. When Prohibition[133] became the law of the land, law enforcement agents began to look for

---

[128] State v. Tanner 745 P.2d 757, 762 n.7 (Or. 1987); State v. Louis, 672 P.2d 708, 710 (Or. 1983).

[129] State v. Campbell, 759 P.2d 1040, 1044 (Or. 1988) (emphasis in original).

[130] Illinois v. Lidster, 124 S. Ct. 885 (2004).

[131] *Id.*, Edmond, 531 U.S. at 32.

[132] The so-called nightwalker statutes in England, beginning with the 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).

[133] U.S. CONST. amend. XVIII (ratified 1919, repealed 1933). Roadway surveillance of course continued even after Prohibition was repealed in 1933 by U.S. CONST. amend. XXI (ratified 1933).

bootleggers transporting illegal alcohol. During this time, the United States Supreme Court upheld a wide range of law enforcement surveillance technologies such as wiretaps aimed at enforcing Prohibition.[134] Stopping bootleggers on the highways to thwart distribution of illegal alcohol was among them.[135]

In the first of the Prohibition-era automobile search and seizure cases, *Carroll v. United States*,[136] the same United States Supreme Court that would later uphold warrantless wiretapping of bootleggers, approved warrantless stopping and searching of cars suspected of containing contraband whiskey. Nevertheless the Court's opinion in *Carroll* took pains to recognize that people on public highways retain certain privacy rights. Chief Justice Taft's opinion for the Court characterized as "intolerable and unreasonable" 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."[137] Chief Justice Taft expressed particular concern about the rights of those 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."[138] Although the Supreme Court held that the particular automobile searches and seizures involved in *Carroll* were lawful, the Court noted that there might well be constitutional objections to wholesale tracking of individuals on public roadways. In other words, following and stopping and searching a particular suspect was permissible. But broad scale surveillance designed to stop everyone on a public road would be "intolerable and unreasonable."

That principle of not allowing government to stop anyone and everyone on the open road continues to play a significant role in evaluating the legality of stopping vehicles on roads and highways. This principle echoes classic notions of limited government[139] in insisting that courts and citizens ought to be skeptical about giving government too much power over individuals. It also reflects concerns about the panopticon effect noted above. Such wariness about the consequences of a too powerful government plays a particularly important role in two recent decisions by the United States Supreme Court in cases involving stopping vehicles on public roads.

The first of these decisions, *Edmond*, involved a narcotics checkpoint seeking to interdict illegal drugs. Police stopped all vehicles passing along a road into Indianapolis, examined each vehicle's exterior with a drug-sniffing dog, but did not search the interiors of the vehicles. The legal context of the *Edmond* decision was somewhat unusual for a search and seizure case, because it involved neither the suppression of evidence in a criminal prosecution nor the so-called automobile exception to Fourth Amendment probable cause requirements for vehicle searches. Rather, *Edmond* was brought as a class action for declaratory and injunctive relief, as well as damages, by two ordinary motorists who had been stopped at the Indianapolis narcotics checkpoint. On behalf of all those stopped at such checkpoints, the plaintiffs challenged the constitutionality of the program that, without any suspicion of wrongdoing, seized their vehicles and themselves.[140] Because the case was brought as a class action for declaratory and injunctive relief, only the general program of stopping vehicles,

---

[134] *See* Olmstead v. United States, 277 U.S. 438 (1928).

[135] Carroll v. United States, 267 U.S. 132 (1925).

[136] 267 U.S. 132 (1925).

[137] *Id.* at 153-54.

[138] *Id.* at 154.

[139] One of the most notable exponents of theories of constitutional limitations was Thomas Cooley, whose A TREATISE ON THE CONSTITUTIONAL LIMITATION was a mainstay of nineteenth century American constitutional theory after the Civil War. THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATION WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION (Boston: Little, Brown, & Co., 1868).

[140] The plaintiffs' request for a preliminary injunction was denied by the United States District Court. But the Seventh Circuit reversed and the United States Supreme Court granted certiorari. The case came before the United States Supreme Court on stipulated facts.

rather than any particular seizure or search of a suspect, was at issue before the Supreme Court. The consequences of protecting the privacy rights of motorists in general in these circumstances were the Court's main focus. "Without drawing the line at roadblocks designed primarily to serve the general interest in crime control, the Fourth Amendment would do little to prevent such intrusions from becoming a routine part of American life," Justice O'Connor ruled.[141] As a routine program of suspicionless seizures by law enforcement agents for general law enforcement purposes, the roadblocks were constitutionally intolerable. Justice O'Connor's opinion for the Court ruled that, because such roadblocks constituted routine suspicionless seizures justified only by the municipality's general interest in crime control, such seizures violated the Fourth Amendment.

The unusual context of this class action which was before the Court on stipulated facts, focused attention on the program of vehicle stops in general, not any particular stop. The six-justice majority struck down such routine narcotics checkpoints along Indianapolis roads as an unconstitutional intrusion. Justice O'Connor's majority opinion emphasizes that the Fourth Amendment's "general rule that a seizure must be accompanied by some measure of individualized suspicion" rendered the roadblock program unconstitutional.[142] "When law enforcement authorities pursue primarily general crime control purposes at checkpoints such as here . . . stops can only be justified by some quantum of individualized suspicion."[143] The opinion does not discuss any particular intrusion caused by the Indianapolis roadblocks at length other than to characterize the interferences as indiscriminate and not based on suspicions of wrongdoing.

Much of the majority opinion in *Edmond* is devoted to distinguishing other types of constitutionally permissible roadblock seizures, such as sobriety[144] and border[145] checkpoints, which the United States Supreme Court has upheld as constitutional. The Court characterized each of these roadblock or checkpoint programs as based on a specific reason or purpose that set each of these particular types of vehicle stops apart from the Fourth Amendment's general proscription that such intrusions are unconstitutional unless based on an individualized suspicion. According to *Edmond*, "The constitutionality of such [other types of] checkpoint programs" require balancing "the competing interests at stake and the effectiveness of the program."[146] But as a general rule, "suspicionless intrusions pursuant to a general scheme" of law enforcement are unreasonable even without balancing the competing interests of the government and individual.[147] What the Court protected in *Edmond* was the general principle that everyone, in particular people on public roads, have constitutionally protected rights to be let alone by the government. Under the Constitution, law enforcement is not normally permitted to routinely stop people on roads and highways without a reasonable suspicion.[148]

---

[141] Edmond, 531 U.S. at 42.

[142] *Id.* at 41.

[143] *Id.* at 47.

[144] Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990).

[145] United States v. Martinez-Fuerte, 428 U.S. 543 (1976). The discretion of border agents to search vehicles for contraband was recently extended in United States v. Flores-Montano, 124 S. Ct. 1582 (2004), which upheld removal and dismantling of a vehicle's fuel tank in searching for illegal drugs at an international border crossing.

[146] Edmond, 531 U.S. at 47.

[147] *Id.*

[148] One interesting feature of the majority opinion is how little it has to say about privacy. Aside from a single reference, when mentioning the Court's earlier decision in Bond v. United States, 529 U.S. 334 (2000) that had recognized a reasonable expectation of privacy with regard to carry-on luggage in the overhead compartment of a bus, the majority opinion does not use the word privacy at all. *Id.* Rather, the opinion discusses such a roadblock as an intrusion, without discussing privacy expectations that a person will not be stopped at a law enforcement checkpoint without a reasonable, focused suspicion that they have done something illegal. An example of a stop based on a reasonable suspicion is the stop in Atwater v. City of Lago Vista, 532 U.S. 318 (2001), an action brought

Edmond insists on the principle that people have the right to be left alone on public roads unless (a) the government has a reasonable suspicion of illegal activity or (b) the government is justified in intruding on everyone because of a particularly vital government program. Without a reasonable suspicion of wrongdoing, intrusions on the privacy of people in public places is presumptively unreasonable and unconstitutional unless one of a very limited set of exceptions applies, such as preventing people from driving under the influence of drugs or alcohol or enforcing immigration laws. The *Edmond* decision articulates a general rule that law enforcement seizures of vehicles are presumptively unreasonable absent a targeted suspicion regarding individual wrongdoing or justification in terms of a critical need, such as controlling illegal immigration or excluding drivers under the influence of alcohol or drugs from highways. Without the peculiar contexts involved in these exceptions, stopping people on public roadways is an unconstitutional seizure.

Chief Justice Rehnquist's dissenting opinion in *Edmond*, joined by Justices Scalia and Thomas, argues for an opposite general rule. According to the dissent, there is no legitimate expectation of privacy that one will not be stopped by the police along public roads. The dissent claims that properly regulated law enforcement roadblock stops of automobiles are presumptively reasonable and result in "only minimal intrusion on the privacy of their occupants."[149] According to the dissent, people in public places should reasonably expect intrusion from government. On public roadways, people can be stopped by law enforcement as a general rule. For this proposition, the dissent relies primarily on two precedents, *Michigan Dep't of State Police v. Sitz*[150] and *United States v. Martinez-Fuerte,*[151] both of which upheld certain roadblocks as constitutional. The dissent asserts that these decisions embody a general rule that roadblock stops are routinely acceptable. These are the very same decisions that Justice O'Connor's majority opinion in *Edmond* carefully distinguishes as exceptions to an opposite general rule that suspicionless roadblock stops are ordinarily not acceptable.

Edmond displays a stark contrast between the views of the majority and those of the dissent regarding whether there is a presumption of privacy on the open road. The majority rules that there is a constitutionally significant intrusion when law enforcement routinely interferes with individuals on public roads. In contrast, the dissent insists that when an individual is on a public road, the Fourth Amendment requires only that the government have a reasonable, nondiscriminatory program for intrusions. At one point the dissent asserts, "The only difference between this case and *Sitz* is the presence of the dog [that sniffed the exterior of the plaintiff's car in *Edmond*]."[152] In a footnote, the majority opinion retorts that the dog-sniff of the exterior of the stopped vehicles is not why the roadblocks are unconstitutional. Rather, "the constitutional defect of the program is that its primary purpose is to advance the general interest in crime control."[153] The fundamental disagreement between the majority and dissent is with regard to whether people in our society can require that law enforcement roadblocks will not, absent limited exceptional circumstances, intrude on them as they travel on public roads. It is not the dog that makes the difference in *Edmond.* What makes the difference is the majority's view that people have a right to be let alone as they travel from place to place. The general rule of the road is that the government will not interfere with law-abiding travelers without a strong justification. Justifications for interferences must be more specific than just a general interest in crime control.

In a separate dissenting opinion, Justice Thomas focused on the issue dividing the majority and dissent -

---

under § 1983 against a law enforcement agency and officer, in which the Court upheld a warrantless arrest of a woman for misdemeanor seat belt violations which the arresting police officer observed. *Id.*

[149] Edmond, 531 U.S. at 48 (Rehnquist, C.J., dissenting). The dissent asserts that roadblocks cause only minimal intrusions on privacy. *See id.* (Rehnquist, C.J., dissenting).

[150] 496 U.S. 444 (1990).

[151] 428 U.S. 543 (1976).

[152] Edmond, 531 U.S. at 52 (Rehnquist, C.J., dissenting).

[153] *Id.* at 44 n.1.

whether or not suspicionless law enforcement stops should be considered a general rule of the road. Justice Thomas's opinion noted that he agreed with the dissent that under *Sitz* and *Martinez-Fuerte*, properly regulated suspicionless roadblock seizures appear to be permitted as a general rule. But Justice Thomas's dissent importantly adds that he is not convinced that *Sitz* and *Martinez-Fuerte* were correctly decided. He suggests that, absent these precedents, the appropriate interpretation of the Fourth Amendment may well be the majority's general rule of privacy on public roads: "Indeed, I rather doubt that the Framers of the Fourth Amendment would have considered 'reasonable' a program of indiscriminate stops of individuals not suspected of wrongdoing."[154] But because the issue of overruling *Sitz* and *Martinez-Fuente* had not been raised, much less briefed or argued, Justice Thomas did not think overruling these decisions was wise in *Edmond.* Justice Thomas's separate dissenting opinion signals that in *Edmond* there was a seventh Justice who believes that, as a general rule, people on public highways should not have to put up with suspicionless roadblocks for general law enforcement purposes.

These issues returned to the Court in *Illinois v. Lidster*,[155] in which the United States Supreme Court upheld the constitutionality of an informational police checkpoint. The Court again reinforced the message of *Edmond* that as a general rule law-abiding motorists have a right not to be stopped for general law enforcement purposes in the absence of a reasonable suspicion of wrongdoing. In *Lidster*, local police had set up an "informational" checkpoint late on a Saturday night to obtain information from motorists about a hit-and-run accident that had resulted in the death of a 70-year-old bicyclist the week before at about the same location and time of night. At the checkpoint, officers stopped each vehicle for 10 to 15 seconds, asked the occupants whether they had seen what had happened there the previous weekend, and handed each driver a flyer describing the accident and requesting information about it. One of the stopped drivers was Lidster whose minivan swerved and nearly hit an officer. Smelling alcohol on Lidster's breath, the officer directed him to an area where another officer administered a sobriety test, after which Lidster was arrested for drunk driving. Convicted of driving under the influence of alcohol, Lidster challenged his conviction on the ground that an illegal checkpoint stop had been used to gather evidence against him in violation of the Fourth Amendment.

The Illinois Supreme Court held that, under *Edmond,* the stop and the arrest that resulted from it were unconstitutional. But the United States Supreme Court upheld Lidster's conviction and distinguished *Edmond* on the grounds that Lidster was detained, not at a general law enforcement checkpoint, but rather at a "brief, information-seeking highway" stop. In these circumstances, the Supreme Court found that the seizure was justified. In making this determination, the Court applied the standards of *Brown v. Texas*,[156] a case that had considered law enforcement questioning of pedestrians.[157] Three justices suggested that the case should have been remanded for the Illinois courts to apply the *Brown* standards.

According to Justice Breyer's opinion for the majority, the importance and effectiveness of police seeking the help of the public in solving a serious crime and the minor delays and lack of intrusiveness caused by the informational checkpoint stop justified the Court's conclusion that the informational stop did not violate the Fourth Amendment. The unanimous Court in *Lidster* explained that "in judging reasonableness, we look to 'the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty.'"[158] These standards are explicitly based on

---

[154] *Id.* at 56 (Thomas, J., dissenting).

[155] 124 S. Ct. 885 (2004).

[156] 443 U.S. 47 (1979).

[157] *Id.* The Court held that "[i]n the absence of any basis for suspecting appellant [Brown] of misconduct, the balance between the public interest and appellant's right to personal security and privacy tilts in favor of freedom from police interference." *Id.* at 52. The Court described three factors to be used in determining that balance: "Consideration of the constitutionality of such seizures involves a weighing of the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty." *Id.* at 50-51.

[158] Lidster, 124 S. Ct. at 890 (quoting *Brown,* 443 U.S. at 51).

Brown[159] where the Court held unconstitutional under the Fourth Amendment the prosecution of a pedestrian in an alley who refused to identify himself to police. In a later decision interpreting *Brown*, the Court explained in *Florida v. Royer,*[160] that the Constitution ordinarily permits police to seek the voluntary cooperation of members of the public in investigating a crime: "[L]aw enforcement officers do not violate the Fourth Amendment by merely approaching an individual on the street or in another public place, by asking him if he is willing to answer some questions, [or] by putting questions to him if the person is willing to listen . . . ."[161] In other words, even though stopping people is a seizure subject to the Fourth Amendment, such stops can be justified when police make simple police inquiries in criminal investigations.

In *Lidster*, Justice Breyer's opinion for the Court reinforces *Edmond's* rulings that "an involuntary stop [of a vehicle] amounts to a 'seizure' in Fourth Amendment terms," and requires that such stops be evaluated with regard to their reasonableness based on the individual circumstances of each stop.[162] Referring to other types of roadblocks allowed under *Sitz* (upholding a sobriety checkpoint) and *Martinez-Fuerte* (upholding a Border Patrol checkpoint), the Court found that the factors suggested in *Brown* also applied to informational police checkpoints. But the Court also made clear "[t]hat does not mean the stop is automatically, or even presumptively, constitutional. It simply means that we must judge its reasonableness, hence, its constitutionality, on the basis of the individual circumstances."[163] This portion of Justice Breyer's opinion for a unanimous Court in *Lidster* seems to settle the debate between the majority and dissent in *Edmond* over the general rule that people on the open road have the right not to be stopped by law enforcement, subject to a few specific exceptions. The general rule of the road remains a right not to be stopped absent a reasonable suspicion of wrongdoing.[164] Justice Breyer's opinion also avoids Justice Thomas's concerns by not overruling *Martinez-Fuerte* or *Sitz*. Rather, Justice Breyer places these decisions upholding certain roadblocks as lawful in a larger context, as Justice O'Connor had done in *Edmond*. In this larger context, roadblocks have to be justified under the standards established in *Brown*.

Together, *Lidster* and *Edmond* suggest that stopping vehicles on roadways is presumptively unconstitutional, but nevertheless subject to a balancing analysis that takes into account the importance of public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of interference with individual liberty.[165] In unanimously ruling that vehicle stops are seizures, the Court endorsed a general rule that people on public roads have a right to be left alone, unless the government has very good reasons for interfering. Although Justice Breyer wryly noted that, "The Fourth Amendment does not treat a motorist's car as his castle," the Court required "special law enforcement concerns" before vehicles can be lawfully stopped.[166] He also held that such concerns would only "*sometimes* justify highway stops

---

[159] *Id*. In Lidster, Justice Breyer's opinion for the Court refers to the ALI, Model Code of Pre- Arraignment Procedure section 110.1(1) (1975) ("[L]aw enforcement officer may . . . request any person to furnish information or otherwise cooperate in the investigation or prevention of crime"), and Haynes v. Washington, 373 U.S. 503 (1963) ("[I]nterrogation of witnesses . . . is undoubtedly an essential tool in effective law enforcement"); as well as U.S. Dept. of Justice, Eyewitness Evidence: A Guide for Law Enforcement 14-15 (1999) (instructing law enforcement to gather information from witnesses near the scene). *Id.*

[160] 460 U.S. 491 (1983).

[161] *Id.* at 497.

[162] Lidster, 124 S. Ct. at 890.

[163] *Id*.

[164] In Atwater v. City of Lago Vista, 532 U.S. 318 (2001), the Court had held that stopping a motorist who was violating seatbelt laws was proper and that she could be arrested and jailed even though her crime was only a misdemeanor. *Id.*

[165] Lidster, 124 S. Ct. at 890.

[166] *Id.* at 889.

without individualized suspicion."[167]

Decisions by state courts regarding vehicle stops have also protected privacy interests of travelers along public roadways. Among the most important is the Pennsylvania Supreme Court decision in *Commonwealth v. Whitmyer*.[168] This suppression of evidence case involved the stop of a motorist who, police alleged, had made erratic lane changes, but had not violated traffic or other laws. The Pennsylvania Supreme Court insisted on "the privacy interest of the individual" in public circumstances. Quoting from the United States Supreme Court's decision in *Delaware v. Prouse*[169] the Pennsylvania Supreme Court noted:

> An individual operating or traveling in an automobile does not lose all reasonable expectation of privacy simply because the automobile and its use are subject to government regulation. Automobile travel is a basic, pervasive, and often necessary mode of transportation to and from one's home, workplace, and leisure activities. Many people spend more hours each day traveling in cars than walking on the streets. Undoubtedly, many find a greater sense of security and privacy in traveling in an automobile than they do in exposing themselves by pedestrian or other modes of travel.[170]

In the search and seizure context, whether with regard to suppression of evidence issues or suits to enjoin government intrusions, privacy along public roadways is generally protected against suspicionless stops.

Being out in public on a highway exposes an individual to being noticed by others, including law enforcement. However, the consequences of allowing law enforcement to stop any vehicle without either suspicion of wrongdoing or special law enforcement concerns runs the risk of overwhelming the privacy rights of individuals with too much social control. Even jurists who describe privacy on the open road as diminished or minimal, do not claim that it is nonexistent. Traditional concerns about curbing the potential for arbitrary exercise of government power apply. As Justice Brandeis noted in a different context, "The makers of our Constitution . . . conferred, as against the Government, the right to be let alone--the most comprehensive of rights and the right most valued by civilized men."[171] Public roads are omnipresent aspects of people's lives. To require a complete waiver of Fourth Amendment privacy interests as an automatic consequence of using them would cede too much control over too important an area of life to government discretion. Other social consequences of on-road activities, such as public safety and solving crime are of course also important. So courts seek a balance that is neither all privacy nor all law enforcement in insisting that when law enforcement stops a vehicle on a roadway, the stop must be based on an important justification.

Open Roads as Open Fields?

Federal Law Regarding Tracking People

Tracking people and vehicles on the road raises very different constitutional issues from the vehicle stops discussed above. Some might even assert that such tracking raises no constitutional issues at all. As a result, modern Fourth Amendment jurisprudence with regard to roadway privacy appears to split right down the middle: On one side, recent United States Supreme Court decisions, discussed above, have made clear that Fourth Amendment protection regarding seizures precludes stopping people and vehicles a highway without sufficient justification. On the other side, the protection regarding searches in that same Fourth Amendment appears to not apply at all when those same people and vehicles are tracked, but not stopped, on those same

---

[167] *Id.* at 889 (emphasis added).

[168] 668 A.2d 1113 (Pa. 1995).

[169] 440 U.S. 648 (1979).

[170] Whitmyer, 668 A.2d at 1117 (quoting Prouse, 440 U.S. at 662).

[171] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (involving wiretapping without a warrant).

highways. This anomaly is worth close examination.

In general, Fourth Amendment limitations on law enforcement agents' tracking, as well as searching, vehicles on public roads are very lenient. This Federal Constitutional tolerance is often expressed in terms of exposure: Information exposed to general public perception appears to be fair game for law enforcement. Even technologically sophisticated surveillance is permitted if law enforcement could have collected similar information by physical surveillance and visual following. When automated technologies, such as GPS, collect much more detailed information than would have been available using visual surveillance, courts usually allow such tracking. They tend to find such tracking it not to constitute a search at all for the purposes of the Fourth Amendment. They typically posit that if, in a perfect world with unlimited numbers of law enforcement agents with keen senses and limitless stamina available, these theoretical law enforcement agents *could* have collected the information by visual surveillance, then law enforcement use of automated surveillance technologies to collect such information is not constitutionally significant. Moreover, because courts often find that there is a diminished expectation of privacy on the part of those in automobiles,[172] the fact that such surveillance is of a vehicle also often helps to justify searching by tracking as legal under federal law.[173]

The Fourth Amendment treatment of tracking vehicles on open roads is an extrapolation of the open fields doctrine articulated by Justice Holmes in *United States v. Hester*,[174] a case involving a jug, a jar and a bottle of illegal moonshine whiskey that were found outside the defendant's father's house: "[T]he special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects,' is not extended to the open fields. The distinction between the latter and the house is as old as the common law."[175] This territorial view of the applicability of Fourth Amendment warrant and probable cause requirements, known as the open fields doctrine, persists despite rejection of place as determinative of Fourth Amendment rights in *Katz*.

The open fields doctrine gradually developed into an open-to-observation standard,[176] although the early rulings did not define what would count as an open field, nor did they involve surveillance. Courts simply ruled that observing something out in the open is a non-event for the purposes of Fourth Amendment search limitations. For example, in *Oliver v. United States*,[177] a case involving outdoor marijuana cultivation behind locked gates and "no trespassing" signs, the United States Supreme Court discussed the open fields doctrine and interpreted it to mean that even when law enforcement agents ignored locked gates and no-trespassing signs that would likely have kept out most members of the public, "government's intrusion upon the open fields is not one of those 'unreasonable searches' proscribed by the text of the Fourth Amendment."[178]

According to the United States Supreme Court in *Florida v. Riley*,[179] a case involving helicopter observations of marijuana cultivation, visual surveillance is permissible to the extent that what was gathered by law enforcement surveillance could also have been seen by the public: "What a person knowingly exposes to

---

[172] Arkansas v. Sanders 442 U.S. 753, 761 (1979) (collects a number of the early cases). *See also* Maryland v. Pringle, 124 S. Ct. 795 (2003); Wyoming v. Houghton, 526 U.S. 295 (1999); United States v. Ross, 456 U.S. 798 (1982); Rakas v. Illinois, 439 U.S. 128 (1978).

[173] The treatment of automobiles as specially justifying searches because they are mobile dates back to Carroll v. United States, 267 U.S. 132, 153 (1925).

[174] 265 U.S. 57 (1924)

[175] *Id.* at 59 (quoting 4 WILLIAM BLACKSTONE, COMMENTARIES * 223, 225-26).

[176] Justice Douglas applied this doctrine in an environmental enforcement case. *See* Air Pollution Variance Bd. of Colorado v. W. Alfalfa Corp., 416 U.S. 861, 865 (1974).

[177] 466 U.S. 170 (1984).

[178] *Id*. at 177 (relying on Hester, 265 U.S. at 57).

[179] 488 U.S. 445 (1989).

the public . . . is not a subject of Fourth Amendment protection."[180] This decision, like many other open fields rulings, does not address roadways, nor does it require that anything had actually been seen by others. Rather it focuses on a hypothetical calculation about what might have been seen, had anyone tried to look. Courts have also ruled that what is theoretically not visible to public view because it is inside a home cannot be surveiled without probable cause and a warrant. In *Kyllo v. United States*,[181] the United States Supreme Court held that warrantless use of infrared sensors to capture patterns of heat generated within a home by marijuana-growing violated the Fourth Amendment. Moreover, even when one is in a public place, the open-to-visual-observation rule does not apply to non-visual surveillance. In *Bond v. United States*,[182] tactile (rather than visual) investigation of a bag in the luggage rack of a public bus was determined to be a search under the Fourth Amendment, even though other people on the bus could also have discovered the contents of the bag by feeling it. The non-visual search was held to be a search under the Fourth Amendment, even though what was searched was out in public on an intercity bus. The search was apparently not subject to the open fields doctrine, which would have made the search a non-event under the Fourth Amendment, because the information collected was non-visual in nature.

The anomalous status of roadway surveillance is largely the result of a pair of United States Supreme Court decisions in the early 1980s involving the use of beepers: *United States v. Knotts* and *United States v. Karo*. These two decisions established that the Fourth Amendment does not generally constrain law enforcement use of electronic tracking devices on the open road. Although the devices at issue in these cases were primitive beepers, the rules set forth in these cases have been applied to all sorts of far more sophisticated tracking devices, such as GPS devices, cell phones and telematics.

In 1983, the United States Supreme Court evaluated law enforcement use of beepers in *Knotts*, in which a beeper was used to snare suspected illegal drug manufacturers. Chief Justice Rehnquist's opinion noted that, in certain instances, pervasive use of such devices on a general basis might become problematic, but concluded that "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[183] After *Knotts*, tracking signals from beepers and transponders has not generally required a warrant, because such tracking is not a search for the purposes of the Fourth Amendment. No such dragnet has been perceived so far.

On occasions when a physical trespass (such as breaking into a garage) is necessary to attach a beeper to a surveillance target's vehicle, some jurisdictions require warrants for the installation of electronic devices.[184] Moreover, in *Karo*,[185] decided a year after the *Knotts* decision, the United States Supreme Court limited the use of tracking devices to areas outside the home. According to the Court's opinion in *Karo*, monitoring a beeper becomes a search under the Fourth Amendment when it reveals "a critical fact about the interior" of a home that could not have been obtained by visual surveillance.[186] This home exception to otherwise lawful technologically enhanced searches was held to be consistent with the outdoors open-to-observation rule noted in

---

[180] *Id.* at 449 (citing California v. Ciraolo, 476 U.S. 207, 213 (1986) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

[181] 533 U.S. 27 (2001).

[182] 529 U.S. 334 (2000).

[183] United States v. Knotts, 460 U. S. 276, 284 (1983). The increasing routine use of tracking technologies described earlier in this article raises questions about whether the growing web of routine roadway surveillance is in fact becoming just such a dragnet.

[184] United States v. Application of the United States for an Order Authorizing the Installation, Monitoring, Maintaining, Repairing, & Removing of Elec. Transmitting Devices & Infra-Red Tracking Devices on or Within a White Ford Truck, 155 F.R.D. 401 (D. Mass. 1994).

[185] United States v. Karo, 468 U.S. 705, 715 (1984).

[186] *Id.* at 715.

its later *Kyllo* decision.[187]

Approval of the use of beepers in tracking criminal suspects on roads and highways appears to follow the following bifurcated analysis: (i) If ordinary physical surveillance could have tracked a vehicle that is outside a house, electronic assistance in following that vehicle does not constitute a search under the Fourth Amendment. (ii) If the vehicle enters a home, tracking it is always a search requiring probable cause and a warrant under the Fourth Amendment. In other words, even when visual surveillance is lost or when sophisticated electronic tracking devices are used in circumstances where visual surveillance is not possible (perhaps because law enforcement agents do not even know the general vicinity of the vehicle or suspect), the open-to-observation rule allows tracking as long as what is tracked remains outside of a home.[188] When the log and recording functions of GPS devices provide different, and far more detailed records than visual surveillance could ever have provided, the same rule that what is out in the open can be tracked by technology continues to be applied by federal courts. For example, in *United States v. McIver,*[189] a case from Montana involving marijuana cultivation in a National Forest, the Ninth Circuit upheld the warrantless placement and use of electronic tracking devices on the undercarriage of McIver's Toyota 4Runner parked in McIver's driveway. The vehicle was then tracked to a marijuana patch in the national forest where automatic cameras photographed the defendant harvesting marijuana.

In the federal courts, just the possibility of being seen, rather than the fact of being seen by law enforcement agents is all that is necessary to avoid Fourth Amendment search restrictions. What law enforcement officials could have perceived with their ordinary senses from and in public locations is not considered a search at all. Camera surveillance of public places is usually justified on this basis as it was in *McIver*.[190] Moreover, the line of cases upholding license plate recognition as not impinging on reasonable expectations of privacy[191] of people on roadways also follows this pattern of analysis.

After the *Knotts* and *Karo* decisions, the Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) amending the original electronic surveillance statute, the Omnibus Crime Control and Safe Streets Act. The ECPA enacted two specific provisions with regard to electronic tracking devices. First, communications from electronic tracking devices (the "I am here" signals) are not protected as "electronic communications."[192] Second, the ECPA added a section (§ 3117) which both defines electronic tracking devices and provides for roving warrants to use such devices outside the jurisdiction of the court authorizing installation of such a device.[193] Subsequent court decisions, discussed above, have held that this statute does not

---

[187] Kyllo, 533 U.S. at 27 (involving use of an infrared device to detect heat patterns in portions of a home used for growing marijuana).

[188] *See, e.g.,* United States v. Forest, 355 F.3d 942 (6th Cir. 2004) (DEA agents repeatedly called a drug dealer's cellular telephone in order to generally locate the suspect within a wide metropolitan area.).

[189] 186 F.3d 1119 (9th Cir. 1999).

[190] *See id.*

[191] However, once a license plate number is connected with an individual, the privacy of the identification information is protected under Driver's Privacy Protection Act, discussed, *infra*. So far, courts in the United States have not yet considered the legality of pervasively tracking vehicle license plate numbers in an effort to track the whereabouts of a targeted individual or individuals. Since the technology to accomplish such tracking is available, use of it to follow the movements of individuals, as well as to identify people whose vehicles were in the vicinity of a particular location, such as a crime scene, is inevitable. Section 215 of the USA PATRIOT Act, enacted in the fall of 2001, after the World Trade Center and Pentagon terrorist attacks, authorizes law enforcement access to a variety of facilities, including license plate readers, and records from them.

[192] 18 U.S.C. § 2510(12)©) (2001).

[193] 18 U.S.C. § 3117.

limit the use of electronic tracking devices, but rather authorizes courts to expand their geographical scope.[194]

State Law Regarding Tracking People on Public Roads

State court decisions are divided on whether a warrant is required to authorize law enforcement use of tracking devices. Some state courts have outright rejected the federal open-to-observation standard in evaluating the legality of law enforcement use of tracking devices. For example, in 1988, the Oregon Supreme Court concluded that "use of the radio transmitter [beeper] to locate defendant's automobile was a search . . . . Because the police did not have a warrant to use the transmitter, and because no exigency obviated the need to obtain a warrant, use of the transmitter violated defendant's rights under Article I, section 9" of the Oregon Constitution.[195] According to the Oregon Supreme Court, the principle that underlies the Oregon Constitution's prohibition against unreasonable searches requires a determination "whether the [beeper] practice, if engaged in wholly at the discretion of the government, will significantly impair 'the people's' freedom from scrutiny."[196] The Oregon Court continued,

> [N]o movement, no location and no conversation in a 'public place' would in any measure be secure from the prying of the government. There would in addition be no ready means for individuals to ascertain when they were being scrutinized and when they were not. That is nothing short of a staggering limitation upon personal freedom.[197]

For the Oregon court, unchecked law enforcement discretion to electronically track people on roadways would result in too much government power over individuals. It was therefore illegal without a warrant.

In contrast, in 2002 the Supreme Court of Nevada approved the warrantless use of an electronic tracking device in a serial rape investigation that led to conviction the defendant's conviction of several offenses, including sex offenses, but not rape. The Nevada Supreme Court flatly concluded, "[W]e can see no objective expectation of privacy in the exterior of an automobile,"[198] and followed the federal open-to-observation approach. The Nevada Supreme Court might have ruled differently, had it agreed with the Oregon Supreme Court that the issue should not be framed in narrow terms of reasonable expectations of privacy, but rather in terms of the consequences of allowing too much power over individuals to be at the discretion of law enforcement agencies. Protecting the rights of citizens against government scrutiny, by requiring a warrant in the absence of a reasonable suspicion of wrongdoing, is an effective way to restrain that power and discretion. But the Nevada Supreme Court was willing to tolerate greater societal control over individuals in the form of law enforcement discretion to use electronic tracking devices.

Some states have enacted specific legislation that restricts the use of tracking devices. As will be discussed more fully below, at least a half dozen states have specific statutes regulating the use of tracking devices. Several of these tracking device statutes, such as legislation in Oregon, Pennsylvania and Utah, establish a court order procedure for the installation and use of tracking devices by law enforcement. But they do not otherwise restrict the use of such devices. Other tracking device statutes, including those enacted by California, Hawaii, Tennessee and Texas sharply restrict the use of such devices, especially for purposes other than law enforcement.

Each statute is somewhat different from the others. A typical state statute is California Penal Code section 637.7, which broadly prohibits "use [of] an electronic tracking device to determine the location or

---

[194] United States v. Gbemisola, 225 F.3d 753 (D. C. Cir. 2000).

[195] State v. Campbell, 759 P.2d 1040, 1049 (Or. 1988).

[196] *Id.* at 1048.

[197] *Id.* at 1049. The Supreme Court of Washington agreed that a warrant was necessary in State v. Jackson, 76 P.3d 217 (Wash. 2003), but found that warrants had been secured in that case. *Id.*

[198] Osburn v. State, 44 P.3d 523, 526 (Nev. 2002).

movement of a person,"[199] without the consent of the registered owner of the vehicle on which the tracking device is installed. In enacting this criminal statute, the California legislature found and declared "that the right to privacy is fundamental in a free and civilized society and that the increasing use of electronic surveillance devices is eroding personal liberty. The Legislature declares that electronic tracking of a person's location without that person's knowledge violates that person's reasonable expectation of privacy."[200] As originally introduced, the proposed legislation prohibited law enforcement use of electronic tracking devices; but, as enacted, the statute contains several exceptions, including one for "the lawful use of an electronic tracking device by a law enforcement agency."[201] The statute defines an "electronic tracking device" as "any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals."[202] In addition to prosecution for a misdemeanor, violations of this statute can be grounds for the revocation of the business licence (e.g. that of a private investigator) of a person or entity illegally using such a device. There are no reported decisions construing California Penal Code section 637.7, although there are occasional press reports of arrests under this statute.[203] The broad reach of the California tracking device statute potentially applies not only to conventional beepers and GPS devices, but also to almost any kind of device that tracks the location of a person or vehicle from one place to another. Even tracking the location of a person through cell phone signals or the DSRC on-board units recently approved by the FCC are potentially within the reach of this statute.[204]

Moreover, other types of state statutes also affect the legality under state law of tracking people on public roads. Many of these statutes do not specifically focus on roadway surveillance, although they may apply in the roadway context. Perhaps the most obvious examples are stalking statutes, which may authorize damage actions as well as establish criminal liability for stalking. Most states have statutes that prohibit stalking. For example, California Civil Code section 1708.7 creates a damage liability for following, alarming or harassing a person who, as a result, fears for his or her safety or that of the person's family.[205] The Civil Code provision requires that the defendant have made credible threats with the intent to cause fear. This statute includes threatening by use of electronic communications - known as "cyberstalking."[206] The counterpart criminal statute is California Penal Code section 646.9, that describes a similar crime of stalking.[207] Such statutes can be used against those who physically follow other people, and could also be applied if on-road surveillance or telematics systems are used to harass or frighten a victim.

Tort Liability for Interference with Privacy On the Open Road

---

[199] CAL. PENAL CODE § 637.7(a) (West 1999).

[200] 1998 Cal. Stat. 499, §1.

[201] CAL. PENAL CODE § 637.7(c).

[202] *Id.* § 637.7(d).

[203] *Police Arrest Suspect in Stalking of Woman*, SAN FRANCISCO CHRON., Apr. 4, 2001, at A16. The article describes the arrest of a 42-year-old man for stalking and unlawfully using an electronic tracking device on a woman's car. The suspect was arrested "after a report of a someone tampering with a car. Officers found a sophisticated tracking device attached to the bottom of the vehicle, police said." *Id.*

[204] See discussion, *supra* at note 59.

[205] *See* CAL CIV. CODE § 1708.7 (West 1998).

[206] *See id.* § 1708.7(b)(2) (West Supp 2004).

[207] CAL. PENAL CODE § 646.9. Ohio statutes contain even more extensive provisions regarding the crime of Menacing by Stalking. OHIO REV. CODE ANN. § 2903.211 (Anderson 1996).

When people track other people on public roads, tort liability is also possible.[208] Although decided cases with regard to such tort liability are fairly few and far between, tort law may apply to vindicate on-the-road privacy, particularly when some of the more advanced tracking technologies discussed in this article are used. Among the distinctive aspects of privacy tort actions is the feature that defendants do not have to have committed a physical trespass onto the plaintiff's property to be liable for invasion of privacy. A person does not necessarily have to be in a private or secluded place to sue for invasion of privacy. Nor is a privacy tort plaintiff required to be aware of the defendant's wrongful actions at the time an invasion of privacy takes place. As a result, the fact that the plaintiff was on a public road, or has not been physically touched by the defendant, or perhaps does not even know about the defendant at the time of the intrusion, does not foreclose liability for invasion of privacy.

Indeed, defendants can be found liable for invading privacy of someone on a public road under each of the four categories of privacy torts outlined in the Restatement, Second, of Torts:[209]

- Unreasonable intrusion upon seclusion, commonly referred to as "Intrusion,"[210]
- Appropriation of another's name or likeness, commonly referred to as "Appropriation,"[211]
- Unreasonable Publicity given to another's private life, commonly referred to as "Public Disclosure,"[212] and
- Publicity unreasonably placing another person in a false light, commonly referred to as "False Light."[213]

The most likely tort actions for invasion of privacy by tracking someone on public roads and highways would be for intrusion and for appropriation of name or likeness.

---

[208] The origins of common law protection for privacy in the United States date back to a famous 1890 law review article, *The Right to Privacy,* largely written by Louis Brandeis, later a United States Supreme Court Justice. Warren & Brandeis, *supra* note 99, at 205. The article described invasion of privacy as interference with an individual's "inviolate personality" and argued that the common law should allow damage actions to redress and punish invasions of privacy. *See id.* at 198, 205. *See also* Glancy, *supra* note 99, at 21-28.

[209] RESTATEMENT (SECOND) OF TORTS §§ 652A-652I (1997) (adopted by the American Law Institute). These four privacy torts are "personal" in the sense that only the living individual whose privacy has been invaded has the right to bring a lawsuit based on them. *Id.* § 652I. Privacy tort actions are generally limited by absolute and conditional privileges similar to those applicable in defamation actions, such as consent and First Amendment protection for freedom of expression. *Id.* §§ 652F-652G. In most cases involving these privacy torts, liability requires the privacy invasion to have been unreasonable.

[210] *Id.* § 652B.

[211] *Id.* § 652C.

[212] RESTATEMENT (SECOND) OF TORTS § 652D.

[213] *Id.* § 652E.

The other two types of invasion of privacy torts - public disclosure[214] and false light[215] - are unlikely to be applicable in many roadway surveillance cases. Both require widespread publicity, not just disclosure or publication to another person as required under the law of defamation. Because both of these privacy torts contemplate media defendants, both are also sharply limited by First Amendment rights. The viability of tort actions against media defendants for public disclosure of private facts is especially questionable after *Florida Star v. B.J.F.*[216] in which the United States Supreme Court made it practically impossible to succeed in such a suit against a media defendant. Similarly, the false light privacy tort has for a long time been on the short list of endangered torts, primarily because publication of false information is actionable as defamation.[217]

Intrusion

The intrusion privacy tort can vindicate a person's seclusion or reserve, even when the person is on a public road. The Restatement describes liability for "Intrusion Upon Seclusion:"

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[218]

This form of invasion of privacy is distinct from other forms of tortious invasion of privacy, because liability for intrusion does not depend on use of information. Rather, it involves interference with autonomy privacy interests.

What makes a defendant liable for intrusion is that the defendant has "invaded a private seclusion that the plaintiff has thrown about his person or affairs."[219] Although the Restatement's discussion of intrusion

---

[214] "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of the kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." *Id.* § 652D. It is possible to imagine cases in which publicity regarding a person's travel patterns collected by traffic surveillance might be actionable. But such actions would be unlikely to be successful because disclosure of information about a person's on-the-road activities is unlikely to be "highly offensive" to a reasonable person. For example, the broadcast of private toll account records showing twice-a-day trips over a particular bridge into another state might constitute a public disclosure of private facts. But just the leaking of the toll records, without publicity about them, would not constitute a public disclosure of private facts, even if the disclosure were highly offensive. Were a newspaper to publish a story containing the records, that would probably be protected as First Amendment activity, unless the story were false. If the feature story were false, then defamation might provide a surer remedy than invasion of privacy.

[215] "One who gives publicity to a matter considering another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed." *Id.* § 652E. One of the early United States Supreme Court decisions approving this aspect of the privacy tort involved a newspaper report of bridge disaster in which a highway fell into a chasm. Cantrell v. Forest City Publ'g Co., 419 U.S. 245 (1974).

One can imagine a case in which a toll tag or license plate recognition system showed a pattern of frequent travel by a car belonging to a religious leader or prominent citizen to and from an area of town known for prostitution or drug sales. The vehicle or toll tag had been used by someone other than the religious leader or prominent citizen. If later, a feature story described the religious leader or prominent citizen as a "known frequenter of the red-light district," such a story could be characterized as a false light invasion of privacy, as well as defamatory.

[216] 491 U.S. 524 (1989).

[217] Diane Leenheer Zimmerman, *False Light Invasion of Privacy: The Light That Failed*, 64 N.Y.U. L. REV. 364 (1989).

[218] RESTATEMENT (SECOND) OF TORTS, *supra* note 209, § 652B.

[219] *Id.* cmt. c.

tends to focus on private places, such as the home,[220] the private seclusion vindicated by this tort is not limited only to the home. The tort explicitly includes protection for the seclusion of people out on the open road: "Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters."[221] The intrusion privacy tort enforces respect for matters that the particular individual reasonably considers personal and secluded. It is important to note that "unless the interference with the plaintiff's seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man," there is no liability for intrusion.[222] Moreover, consent can also be a determinative issue in intrusion cases.[223]

Court decisions have recognized that people on public roadways have rights to vindicate intrusions on their privacy. Perhaps the most famous of these intrusion decisions is *Galella v. Onassis*[224] in which a federal district court granted injunctive relief against a celebrity photographer (self-described as a "paparazzo," named after an annoying insect) who had followed, photographed and harassed Jacqueline Kennedy Onassis and her children in public places such as streets, sidewalks and pathways. Ultimately, the Second Circuit Court of Appeals modified the injunction so as not to interfere with proper news coverage of the late President's wife and children.[225] But the district court's finding of tortious intrusion on Mrs. Onassis and her children in public settings as an appropriate basis for injunctive relief remained unaffected. Even though she chose to go out on the open road with her family, Mrs. Onassis did not impliedly consent to Galella's intrusions on her privacy.

An earlier court decision based on intrusion protected the public activities of Ralph Nader. In *Nader v. General Motors Corp.*,[226] the New York Court of Appeals upheld against a motion to dismiss, Ralph Nader's complaint that agents of General Motors shadowed and kept him under surveillance, both physical and electronic, tracking him as he moved about on public roads and in public places. The court noted, "A person does not automatically make public everything he does merely by being in a public place . . . ."[227] These cases, and others like them, stand for the proposition that persons in public settings, such as roadways, retain privacy rights vindicated by the intrusion tort.

Fairly egregious facts tend to characterize cases in which plaintiffs have prevailed in intrusion privacy actions arising out of public roadway settings. After all, to be actionable under the Restatement, an intrusion must be "highly offensive to a reasonable person." For example, in *Wolfson v. Lewis*,[228] a federal district court issued a preliminary injunction against television reporters who shadowed the family of executives of a

---

[220] For example, the comment notes that wrongful intrusion does not ordinarily extend to observing or even taking the photograph of a plaintiff "while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye." *Id.*

[221] *Id.* The illustration provided for the latter point is a photograph taken in an amusement house of a young woman whose skirts have been blown over her head by a concealed jet of compressed air. *Id.* illus. 7.

[222] RESTATEMENT (SECOND) OF TORTS, *supra* note 209, § 652B cmt. d.

[223] *Id.* § 652F cmt. b.

[224] Galella v. Onassis, 353 F. Supp. 196 (S.D.N.Y. 1972) *modified by* 487 F.2d 986 (2d Cir. 1973).

[225] Galella v. Onassis, 487 F.2d 986 (2d Cir. 1973). The modified injunction continued to prohibit approaching with in twenty-five feet of Mrs. Onassis "blocking of her movement in public places and thoroughfares," and any actions that would put her health and safety in jeopardy or would be likely "to harass, alarm or frighten" her. *Id.* at 998.

[226] 255 N.E.2d 765 (N.Y. 1970).

[227] *Id.* at 771. The court noted that there would be no intrusion into plaintiff's "private sphere" when "the plaintiff acted in such a way as to reveal that fact to any casual observer." *Id.* Activities and details not observable by casual observers were subject to legal protection against intrusion.

[228] 924 F. Supp. 1413 (E.D. Pa. 1996).

healthcare insurer.[229] Surveillance took the forms of closely following automobiles in which the executives or their families went to school or to work, and of using remote cameras, parabolic microphones and the like. The potential for violence, as security and safety fears mounted, prompted the judge to describe the defendants' actions as "hounding, harassing, intimidating and frightening conduct."[230] The court expressed particular concern about the "intrusion upon seclusion . . . by electronic means such as wiretapping, photography or the use of binoculars."[231] The fact that the intrusions had taken place in public did not undercut the plaintiffs's claims based on invasion of privacy by intrusion.

In a somewhat different type of case, *Hidey v. Ohio State Highway Patrol*,[232] an Ohio Court of Appeals found a viable intrusion upon seclusion privacy claim on the part of a female passenger asked to leave a vehicle that had been stopped for speeding alongside an interstate highway. While the passenger stood along side the highway, the officer shined a flashlight down the front and back of her pants and then told her to partially disrobe in the back of the cruiser. The court ruled that, "What is underneath her clothing is private and a part of appellant's seclusion. The intrusion upon these private matters, especially while on the side of an interstate highway, would be highly offensive to a reasonable person . . . ."[233] To the extent that routine traffic surveillance, whether by cameras or other electronic equipment, results in similar outrageous exposure, the tort of intrusion may well apply to vindicate the privacy of people along public roads and highways.

One of the most interesting recent decisions upholding liability for intrusion in a highway setting is *Shulman v. Group W Prods., Inc.*[234] The case involved several types of privacy claims brought by automobile accident victims who, without their consent, were featured in a television report about the accident in which the plaintiffs were very badly injured. Although the decision in the case is complicated by multiple opinions and shifting majorities, the majority opinion's discussion of the intrusion tort "expresses the views of a majority of the court's members."[235] In finding that, "It is in the intrusion cases that invasion of privacy is most clearly seen as an affront to individual dignity,"[236] the majority opinion quoted at length from the late Professor Edward Bloustein, who had warned,

> "[A] measure of personal isolation and personal control over the conditions of its abandonment is of the very essence of personal freedom and dignity, is part of what our culture means by these concepts. . . . He who may intrude upon another at will is the master of the other and, in fact, intrusion is a primary weapon of the tyrant."[237]

Although the court did not consider the accident scene (a ravine off the highway) to be private, the court found "two triable issues of intrusion on seclusion."[238] First, the court found an "objectively reasonable expectation of privacy" with regard to the interior of the rescue helicopter, which the court analogized to an ambulance or

---

[229] *Id.*

[230] *Id.* at 1433.

[231] *Id.* at 1434.

[232] 689 N.E.2d 89 (Ohio Ct. App. 1996).

[233] *Id.* at 93.

[234] 955 P.2d 469 (Cal. 1998).

[235] *Id.* at 475 n.2.

[236] *Id.* at 489.

[237] *Id.* (quoting Bloustein, *supra* note 100, at 973-74).

[238] *Id.* at 490.

hospital room.[239] Second, the court found a protectable privacy interest in the conversations between one of the accident victims and medical rescuers. Noting that there are no bright lines with regard to such questions, the court held that the determination whether newsgatherers "acted with highly offensive disrespect for . . . personal privacy" in intrusion cases should be determined by juries in California.[240]

In a later case involving intrusion, a unanimous decision of the California Supreme Court approved protection of privacy expectations against intrusion in another type of public setting, an office.[241] The court emphasized two required elements for an intrusion cause of action: "(1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person."[242] The first element requires that a plaintiff have a reasonable expectation of privacy, but does not require such a privacy expectation to be "of absolute or complete privacy."[243] The court explained that for the purposes of the intrusion tort, there can be enforceable expectations of limited privacy in public settings. The court explained that privacy "is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law."[244]

Quoting from Professor Thomas McCarthy, the court noted that, "'Like 'privacy,' the concept of 'seclusion' is relative. The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone.'"[245] The court noted that determining whether an area is one of limited seclusion is properly a factual issue for a jury or other fact-finder to decide. In intrusion cases, "the reasonableness of a person's expectation of visual and aural privacy depends not only on who might have been able to observe the subject interaction, but on the identity of the claimed intruder and the means of intrusion."[246] The court also noted that, "We do not suggest that the same standards necessarily apply to private intrusions as to government searches, or vice versa."[247] According to the California Supreme Court, the notion of reasonable privacy expectations in tort law is distinct from the contentious reasonable expectation of privacy concepts under federal search and seizure law.

Whether routine surveillance of activities along public roads would rise to the level of tortious intrusion is uncertain. What is likely is that intrusion cases brought in California will often withstand demurrer and summary judgment motions. They are likely to be ultimately decided by juries in California. Particularly egregious factors, such as using a traffic surveillance camera to capture activities in buildings adjacent to the roadway or to peer into vehicles and perhaps look at a driver's clothing or lack thereof, or at the emotional state of passengers in vehicles or at the text of their reading materials, could be types of roadway surveillance that might well result in liability. Under the standards established for intrusion actions by the California Supreme Court, it would be up to a jury to decide whether the context was sufficiently private and whether the intrusion was highly offensive.

---

[239] Shulman, 955 P.2d at 490.

[240] *Id.* at 494-95.

[241] Sanders v. ABC, 978 P.2d 67 (Cal. 1999) (involving an investigative reporters use of a hidden microphone and camera in investigating a telepsychic business from inside the offices of that business).

[242] *Id.* at 71.

[243] *Id.*

[244] *Id.* at 72.

[245] *Id.* (quoting THOMAS J. MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5.10(A)(2) (2d ed. West Group 2000)).

[246] Sanders, 978 P.2d at 77.

[247] *Id.* at 74 n.3.

Appropriation

Privacy rights to prevent appropriation of an individual's name or likeness[248] can apply to people in vehicles. In *Motschenbacher v. R.J. Reynolds Tobacco Co.,*[249] the Ninth Circuit held that legal protection for "an individual's proprietary interest in his own identity," was available when a cigarette company used distinctive features of a famous race car driver's vehicle in a television commercial for cigarettes without the car owner's permission.[250] Even though the appearance of the race car was slightly altered, its distinguishing features were still apparent. These features caused viewers to believe that the car was being driven by the celebrity race car driver, who was in fact in the car when the altered photograph was taken but was not visible in the photograph.

When vehicles, or their travel patterns, are similarly associated with particular persons, and such things are used for advertizing purposes, there appears to be potential liability for the appropriation of personal identity. Most of the reported court decisions regarding tort liability for invasion of privacy by appropriation involve commercial use of a person's name or likeness in advertising. For example, liability for appropriation might result from the image of a vehicle driver or perhaps of a bicyclist or pedestrian, captured by a remote camera or photo radar, when the image was later used in commercial advertizing without the consent of the person involved.

The law enforcement surveillance systems described above are not now used to collect or to distribute information for advertizing purposes. But some of the advanced ITS technologies, particularly those involving vehicles equipped with location devices and on-board communication units, make it possible to collect a data image of an individual's movements and decisions, sometimes called a user profile. Such a data profile has substantial commercial value. Because these data images or user profiles of travel patterns are extremely valuable for marketing purposes, there have been a number of suggestions for applying the appropriation privacy tort to data collection.[251] For example, Professor Andrew McClug has made an extended argument for applying the appropriation privacy tort in situations involving dossiers of consumer data, data mining and consumer profiling.[252] He suggests focusing on appropriation rights that vindicate the identity and personal dignity rights of non-famous ordinary individuals. After all these appropriation cases vindicate interference with individual self-determination, and are fundamentally different from the property-based actions that vindicate celebrities's ownership of their publicity rights.[253] In the non-celebrity cases, individual identity and

---

[248] *See* RESTATEMENT (SECOND) OF TORTS, *supra* note 209, § 652C.

[249] 498 F.2d 821 (9th Cir. 1974).

[250] *Id.* at 825.

[251] Recent scholarly writing asserts ownership of information derived from individuals. For example, in *The Architecture of Privacy*, Professor Lawrence Lessig maintains that people own data of which they are the subject, or source. Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56 (1999). His widely-acclaimed book, CODE AND OTHER LAWS OF CYBERSPACE, makes a similar argument. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999). However, aside from particular legislation requiring individual consent to the use of certain types of information about a person and tort rights protecting the publicity rights of celebrities, United States law has up to now not often recognized such ownership theories. Other academic lawyers, such as Professor Pamela Samuelson, have argued that control over information about a person is better protected through a licensing system, similar to that which applies regard to trade secrets. *See* Pamela Samuelson, *Privacy as Intellectual Property?,* 52 STAN. L. REV. 1125 (2000). Even academic speculation has tended to stop short of asserting privacy rights to refuse participation in anonymous data collection. *See also* Janet Dean Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943 (2002); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000).

[252] Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63 (2003).

[253] The United States Supreme Court approved such an appropriation right for a person who performed a human canon ball act in Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562 (1977). *See, e.g.,* Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988); Estate of Presley v. Russen, 513 F. Supp. 1339 (D.N.J. 1981).

dignity rights can be vindicated by the appropriation privacy tort.[254] Such rights associated with autonomy privacy interests can also be infringed by mass data collection, data mining and consumer profiling. Such appropriation privacy tort protections may also apply to the personal travel patterns of individuals captured by advanced roadway tracking systems described in this article. Legislative recognition that ordinary individuals have such privacy rights that include proprietary control over information about their driving patterns is evidenced in the vehicle "black box" legislation discussed below.[255]

State Constitutional Privacy Guarantees

Aside from protections against unreasonable searches and seizures[256] discussed above, Federal Constitutional law does not offer general privacy protections against roadway surveillance. Nor has the United States Constitution been applied to restrict gathering or use of personal information.[257] However, state constitutional law is quite different. In fact, some state constitutions offer important protections for the privacy of people on the open road. About ten state constitutions contain provisions expressly guaranteeing a right of privacy.[258] Other state constitutions have been interpreted to contain an implied privacy right.[259] Many of these state constitutional privacy protections apply to both public and private sector entities,[260] as well as to both collectors and transferees of personal information. So far, these specific constitutional privacy guarantees have not yet been applied to tracking people on roadways, although state constitutional restrictions against unreasonable searches and seizures are the basis for restricting the use of tracking devices discussed above.[261]

It may be useful to point out that at least one type of out-in-the-open roadway-related activity has been protected by some state constitutional privacy rights. That activity is leaving trash on the curbside for removal by sanitation workers. The United States Supreme Court does not recognize privacy rights in trash left on the curbside to be removed by refuse collectors.[262] But several state supreme courts have protected such privacy rights as a matter of state constitutional privacy law.[263] These cases might be extended from trash on the roadside to cars on the roadway, for example, when remote highway sensors are used to collect data about vehicle tailpipe emissions.

The California constitutional protection for privacy was among the earliest of these state constitutional privacy provisions. For over thirty years, the Constitution of the State of California has explicitly guaranteed an "inalienable right to privacy" in Article I, §1. This constitutional privacy right was adopted in a 1972 initiative

---

[254] RESTATEMENT (SECOND) OF TORTS section 652C explains in comment b that appropriation liability "is not limited to commercial appropriation. It applies also when the defendant makes use of the plaintiff's name or likeness for his own purposes and benefit, even though the use is not a commercial one, and even though the benefit sought to be obtained is not a pecuniary one." RESTATEMENT (SECOND) OF TORTS, *supra* note 209, § 652C cmt. b. Three of the illustrations involve impersonation. *See id.* illus.

[255] *See* discussion *infra* note 322.

[256] *See* text discussion *supra* notes 130-66.

[257] Paul v. Davis, 424 U.S. 693 (1976).

[258] These states include Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and West Virginia.

[259] These states include Arkansas, New Hampshire, New Jersey, and perhaps Iowa.

[260] The Alaska, California, Hawaii, Illinois, and Louisiana constitutions provide that their privacy guarantees apply to private-sector as well as public-sector invasions of privacy.

[261] *See* discussion *supra* notes 195-97.

[262] California v. Greenwood, 486 U.S. 35 (1988).

[263] The states in which state constitutional privacy rights protect privacy in these circumstances include California, Hawaii, New Jersey, Washington, and perhaps Indiana, where the intermediate appellate courts are divided on the issue.

campaign in which concerns about collection and misuse of information about individuals were prominent reasons for the measure's adoption. Because under California law ballot arguments are used to interpret legislative intent with regard to initiative measures, it is useful to consider the potential application of this constitutional privacy right to collection and use of information about people's activities on the open road:

> The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. . . . The average citizen also does not have control over what information is collected about him. Much is secretly collected . . . . Modern technology is capable of monitoring, centralizing and computerizing this information which eliminates any possibility of individual privacy. [California's Constitutional privacy right is designed to] prevent misuse of this information for unauthorized purposes and preclude the collection of extraneous or frivolous information.[264]

Under this Constitutional provision, both public-sector and private-sector interferences with privacy are lawful only if they are justified by a very important societal interest. Whether combating traffic congestion, or collecting travel patterns of everyone who takes a certain route, or locating potential terrorist suspects would qualify as such very important societal interests has not yet been decided.

No reported decision has directly addressed the application of this constitutional privacy right to roadway surveillance. But the California Supreme Court has enforced this constitutional privacy right in the context of surveillance of public activities. In *White v. Davis*[265] the California Supreme Court upheld a taxpayer's complaint, brought under California Civil Procedure Code section 526a, seeking an injunction against expenditure of public funds for covert police surveillance of university classes and other public activities at the University of California at Los Angeles.[266] Justice Tobriner presented the case as raising two questions:

> [First:] Do the state and federal Constitutions permit police officers, posing as students, to enroll in a major university and engage in the covert practice of recording class discussions, compiling police dossiers and filing "intelligence" reports, so that the police have "records" on the professors and students? [Second:] Is this "intelligence gathering" by the police covering discussions in university classes and in public and private meetings of university-sponsored organizations, constitutionally valid when such reports "pertain to no illegal activity or acts"?[267]

The answer to each of these questions was a resounding "no." Only a showing of compelling state interest could justify such a surveillance regime.

Perhaps the court's sharp reaction to the surveillance in *White* was affected by factual allegations that included: "extensive, routine, covert police surveillance of university classes and organization meetings" that the court described as "unprecedented in our nation's history."[268] But the court also pointed to "routine stationing of covert, undercover police agents in university classrooms and association meetings, both public and private." The Court held that such routine surveillance "constitutes 'government snooping' in the

---

[264] PROPOSED AMENDMENTS TO CONSTITUTION- PROPOSITIONS AND PROPOSED LAWS TOGETHER WITH ARGUMENTS - GENERAL ELECTION, TUESDAY, NOVEMBER 7, 1972, at 27, 28.

[265] 533 P.2d 222 (Cal. 1975).

[266] *Id.* at 226.

[267] *Id.* at 224.

[268] *Id.* at 235.

extreme."[269] Since it was alleged "that the information gathered by the undercover agents from class discussion and organization meetings 'pertains to no illegal activity or acts,'" the court surmised "that the gathered material, preserved in 'police dossiers,' may be largely unnecessary for any legitimate . . . governmental interest."[270] Whether similar covert collection of information (e.g., dossiers in the form of itineraries) of law-abiding people on the open road would evoke a similar response has yet to be decided.

In a later decision interpreting the California state constitutional privacy guarantee, the court reaffirmed that the California constitutional right to privacy applies broadly to all sorts of both governmental and nongovernmental actors - Big Brother and Big Sister from the public sector, as well as the little-brothers from the private sector. In *Hill v. NCAA,*[271] the California Supreme Court sharply distinguished the circumstances in *White* and ruled that most California state constitutional privacy actions against nongovernmental privacy invasions simply require a balancing of competing societal interests. The California Supreme Court also provided guidance for such balancing in outlining the elements of a cause of action for invasion of the state constitutional right to privacy: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy."[272] The decision also recognizes defenses to this cause of action in the form of competing interests that derive from "legally authorized and socially beneficial activities of government and private entities."[273] Enforcing the California constitutional right to privacy can present a fairly daunting task for plaintiffs who seek to fulfill each of these requirements.

With regard to showing a legally protected privacy interest, it is useful to bear in mind that the California Supreme Court explained in *Hill*, *supra*:

> Whatever their common denominator, privacy interests are best assessed separately and in context. Just as the right to privacy is not absolute, privacy interests do not encompass all conceivable assertions of individual rights. Legally recognized privacy interests are generally of two classes: (1) interests in precluding the dissemination or misuse of sensitive and confidential information ("informational privacy"); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ("autonomy privacy").[274]

As noted above, roadway surveillance potentially affects both types of legally protected privacy interests. These interests involve both information privacy interests in precluding misuse of information regarding one's location, as well as autonomy interests in not having one's activities on the road scrutinized and information about them collected without one's consent. The court in *White* was particularly concerned about the ways in which surveillance of public activities affects autonomy interests and can affect, and sometimes chill, personal decisions.

In the context of ITS, information collected by roadway surveillance in the form of anonymous traffic flow information used in traffic management does not involve personally identifiable information at all. Such information only becomes personally identifiable when it is associated with a vehicle owner through a vehicle license plate or a toll tag identifier. A comprehensive data could of course connect an identified individual's

---

[269] *Id.* at 234.

[270] White, 533 P.2d at 234.

[271] 865 P.2d 633 (Cal. 1994) (upholding drug testing of student athletes under an NCAA anti-drug program).

[272] *Id.* at 675.

[273] *Id.* at 656.

[274] *Id.* at 654.

itineraries with other types of information about the individual -- such as name, address, social security number, purchases with credit cards, law enforcement information, other locations visited, and information about associates. In such circumstances, the California state constitution would probably be interpreted to recognize a much stronger privacy interest.

Second, under *Hill*, a cause of action for invasion of the state constitutional right to privacy also requires a reasonable expectation of privacy under the circumstances. As, the California Supreme Court explained in *Hill*, "A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms."[275] Among the "customs, practices, and physical settings surrounding particular activities" that "create or inhibit reasonable expectations of privacy," the court notes particularly "the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests."[276] As a result, the open circumstances of travel on public roads might appear to signify a sort of implied waiver of privacy expectations.[277] And yet even though most travel activities on the open road are open to observation, constitutionally protected expectations of privacy have been protected even in relatively open places. For example, in a public university in *White*[278] an in a public office in *Sanders*,[279] the impact of the surveillance on individual privacy was determined to be too great.

The third element of a cause of action for interference with the California state constitutional right to privacy requires that, "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right."[280] As the California Supreme Court noted in *Hill*, "No community could function if every intrusion into the realm of private action, no matter how slight or trivial, gave rise to a cause of action for invasion of privacy."[281] With regard to roadway surveillance, social norms regarding collection of information about individuals are only beginning to emerge. In some cases, such as roadway stops, the norms seem to be clear. But in other types of cases, particularly with regard to technologically advanced surveillance that tracks people on public roadways, the public norms are much less clear. One source of privacy norms applicable to roadway surveillance would be the privacy principles of the Intelligent Transportation Society of America discussed above.[282]

Even when a cause of action for interference with the state constitutional right to privacy has satisfied the above three elements, there remains an opportunity to again balance privacy interests against competing societal interests. This balancing occurs through the defenses discussed at length in *Hill*:

> The diverse and somewhat amorphous character of the privacy right necessarily requires that privacy interests be specifically identified and carefully compared with competing or countervailing privacy and nonprivacy interests in a "balancing test." The comparison and balancing of diverse interests is central to the privacy jurisprudence of both common and

---

[275] *Id.* at 655.

[276] Hill, 865 P.2d at 655.

[277] For example, in People v. Stanley, 86 Cal. Rptr. 2d 89 (Cal. Ct. App. 1999), the District Court of Appeal held that there was no reasonable expectation of privacy in the amount of electricity entering a person's home that was measured surreptitiously by a box installed by the electric company on a public utility pole outside the defendant's house. *Id.*

[278] White, 533 P.2d at 222.

[279] Sanders v. ABC, 978 P.2d 67 (Cal. 1999) (also an intrusion privacy tort action).

[280] Hill, 865 P.2d at 655.

[281] *Id.*

[282] *See* discussion *supra* note 107.

constitutional law.[283]

Various types of roadway surveillance would involve balancing different competing societal purposes: Law enforcement roadway surveillance systems serve traffic and law enforcement purposes. ITS traffic management systems serve such societal interests as traffic safety, environmental protection, as well as preventing traffic congestion. Some of the private-sector telematics systems may serve less weighty societal interests, such as consumer convenience, advertising and the like. Such interests would be balanced along with the privacy interests in determining whether there is too much societal control over the individual.

Two related factors - lack of choice and government coercion - tend to tip the balance toward a finding of unconstitutional privacy interference. The California Supreme Court has repeatedly insisted on the importance of choice:

> If, for example, a plaintiff claiming a violation of the state constitutional right to privacy was able to choose freely among competing public or private entities in obtaining access to some opportunity, commodity, or service, his or her privacy interest may weigh less in the balance. In contrast, if a public or private entity controls access to a vitally necessary item, it may have a correspondingly greater impact on the privacy rights of those with whom it deals.[284]

When ITS traffic management systems collect origin-destination data without the knowledge or consent of the person being tracked, the person is deprived of any choice. On the other hand, if drivers can choose to travel toll roads anonymously, as is the case with regard to certain Canadian toll roads,[285] choice is restored. When travelers are informed about the collection of origin-destination data and given the opportunity to consent or not to the use of data about their travels, privacy interferences are mitigated. Moreover, the California Supreme Court has expressed repeated concern that "the pervasive presence of coercive government power in basic areas of human life typically poses greater dangers to the freedoms of the citizenry than actions by private persons."[286] When law enforcement agents surreptitiously attach a tracking device to a vehicle, coercive government action causes increased concern about privacy.

Aside from forming the basis for litigation against both public-sector and private-sector invasions of privacy, the California Constitutional privacy guarantee has also played a role in forestalling efforts to gain discovery of personal location information. For example in *Planned Parenthood Golden Gate v. Superior Court,*[287] Justice Haerle held that the state constitutional right to privacy outweighed the interest in requiring disclosure of the names and residential addresses of Planned Parenthood's staff and volunteers who were not parties to the litigation. The litigation was over anti-abortion protestors's rights to protest outside an abortion-provider's facility. The court found that "a privacy interest does not need to be violated before it can be acknowledged. . . . [R]ecent history teaches that the consequences of disclosure of private information about these individuals can be dire."[288] In response to a suggestion that "individuals do not have strong privacy interests in their residential addresses and telephone numbers because such information is routinely disclosed during discovery and is often accessible by other means," Justice Haerle replied that in the particular context at

---

[283] *Hill*, 865 P.2d at 655.

[284] *Id.* at 657.

[285] *See, e.g.*, *407 Toll Route: How You Can Travel the 407 Anonymously*, Information and Privacy Commissioner website, *at* http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=11353&U_ID=0 (last visited Aug. 11, 2004).

[286] Hill, 865 P.2d at 656.

[287] 99 Cal. Rptr. 2d 627 (Cal. Ct. App. 2000).

[288] *Id.* at 640.

issue there was "a very strong privacy interest in avoiding disclosure."[289]

As discussed above, all state constitutions specifically prohibit unreasonable searches and seizures. In some instances courts have found state constitutional protections against warrantless searches and seizures to prohibit use of electronic tracking devices without a warrant.[290] The Oregon Supreme Court even found that the Oregon constitution protects "freedom from scrutiny."[291] Similarly, the Washington Supreme Court concluded "that the citizens of this State have a [constitutional] right to be free from the type of governmental intrusion that occurs when a GPS device is attached to a citizen's vehicle, regardless of reduced privacy expectations due to advances in technology."[292]

Statutes Restricting Roadway Surveillance

Concerns about privacy on the open road have generated a remarkably varied group of statutes that address particular privacy problems posed by specific types of roadway surveillance. Categorizing these statutes is difficult because the legislation tends to respond to particular concerns about potential invasions of privacy by specific types of technology. Because federal statutes apply more widely than the legislation of any one state, it makes sense to first discuss some of the relevant federal legislation and then turn to some of the much more numerous and various state statutes.

Federal Statutes

The original legislation that established the Intelligent Transportation Systems program required the program to be developed in light of concerns about privacy.[293] The United States Department of Transportation, through the Federal Highway Administration and the ITS Joint Program Office continues to support and to fund ITS programs in the spirit of this mandate. Not only is federal funding for ITS projects typically contingent on properly taking account of privacy; in addition, the Intelligent Transportation Society of America (formerly the designated advisory committee to the Department of Transportation on ITS issues) developed the privacy principles noted earlier which the Society recommends be followed by all of its members.[294] As a result, recognition of privacy interests are woven into almost every aspect of ITS programs.

At a more specific level, the federal Driver's Privacy Protection Act[295] (DPPA) restricts state departments of motor vehicles, and others who sell and disclose information from state departments of motor vehicles databases, from disclosing personal information about a driver without the driver's consent. The United States Supreme Court unanimously upheld this privacy mandate against a federalism challenge based on the Tenth and Eleventh Amendments in *Reno v. Condon*.[296] The Supreme Court ruled that the Driver's Privacy Protection Act was legislation of general application that "regulates the universe of entities that participate as suppliers to the market for motor vehicle information -- the States as initial suppliers of the information in

---

[289] *Id.* at 641, 643. In vacating the trial court's discovery order, the Court of Appeal even rejected the use of a protective order with regard to private data identifying the location of individuals. *Id.* at 645.

[290] *See* discussion *supra* notes195-97.

[291] State v. Campbell, 759 P.2d 1040, 1048 (Or. 1988)

[292] State v. Jackson, 76 P.3d 217, 224 (Wash. 2003).

[293] Pub. L. No. 102-240, 105 Stat. 2189, § 6054. *See* Norman Y. Mineta, *Transportation, Technology and Privacy*, 11 SANTA CLARA COMPUTER & HIGH TECH. L. J. 3 (1995).

[294] *See* discussion *supra* note 107.

[295] 18 U.S.C. §§ 2721-2725 (2001).

[296] 528 U.S. 141 (2000).

interstate commerce and private resellers or redisclosers of that information in commerce."[297]

The DPPA restricts the availability of personal information identifying an individual without the consent of the individual. Personal information protected under the statute includes information that identifies an individual, such as "an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code) telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status."[298] An even more carefully protected category of "highly restricted personal information" includes the "individual's photograph or image, social security number, medical or disability information."[299] Specific provisions restrict the use and disclosure of such information both by state motor vehicle licensing authorities and by those who use information derived from official driver's license records. The DPPA specifically restricts reuse of information about drivers that was collected for licensing purposes. Without the written consent of the driver, information about a driver cannot be used for other purposes. Passage of the statute was stimulated in part by notorious cases of stalkers who murdered victims whose addresses had been obtained through requests for DMV records.[300]

In addition, federal electronic surveillance laws protect the content of wireless communications to and from vehicles against unlawful interception. Special procedures are established for law enforcement and intelligence agencies to access these communications under specified circumstances.[301] The USA PATRIOT Act, noted above, has significantly expanded the ability of law enforcement and intelligence agencies both to intercept the content of communications through electronic surveillance and to access a wide variety of business records, such as those containing location information held by communications providers.

Because the United States Supreme Court held in *Smith v. Maryland*, 442 U.S. 735, 740 (1979) that restrictions on electronic surveillance did not apply when the government used a pen register to record numbers dialed from a telephone, no warrant is required for similar interceptions of to-from information in the context of wireless communications. Moreover, as noted above, in 1986 the Electronic Communications Privacy Act exempted electronic tracking devices from the restrictions on electronic surveillance in 18 U.S.C. § 2510 and added 18 U.S.C. § 3117 to specifically authorize courts to permit use of electronic tracking devices beyond the court's geographical jurisdiction. As noted earlier, this section places few restraints on the use of electronic tracking devices and simply recognizes courts's authority to permit the monitoring of these devices across jurisdictions.

The potential for tracking the locations of wireless communications devices some of which are attached to or carried in vehicles, caused Congress to require that automatic location identification (ALI) not be used for tracking wireless communications device users, other than for emergency response purposes.[302] A separate statute, the Communications Assistance for Law Enforcement Act, 18 U.S.C. § 2522 and 47 U.S.C. §§ 229, 1001-1010, facilitates law enforcement access to this location information.[303] Indeed, Congressional concerns about potential misuse of automatic location identification (ALI) are reflected in 47 U.S.C. § 222 designed to

---

[297] *Id.* at 151.

[298] 18 U.S.C. § 2725(3).

[299] *Id* § 2725(4).

[300] According to Senator Barbara Boxer, The Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725, was prompted by the 1989 murder of actress Rebecca Schaeffer, star of the hit television series, "My Sister Sam." *See* 139 CONG. REC. S15745-01, 515762 (1993) (statement of Sen. Boxer). But there were other notorious cases as well. *See also* Ellen Barry, *Killer's Dreams Bared on the Internet N.H. Man Took to Web to Boast and to Stalk*, BOSTON GLOBE, Nov. 29, 1999, at B1.

[301] 18 U.S.C. § 2510.

[302] 47 U.S.C. § 222 (2001).

[303] Cell phone records have been successfully used as evidence in criminal cases. United States v. Forest, 355 F.3d 942 (6th Cir. 2004).

protect the privacy of location information obtained by wireless carriers. Federal law protects this location information against disclosure by wireless carriers both generally under § 222(a)[304] as well as under § 222(c) as customer proprietary network information (CPNI).[305] However, the precise meaning of this privacy protection remains somewhat opaque after the Tenth Circuit Court of Appeals struck down FCC rules interpreting the statute to require affirmative choice (opt-in) by subscribers regarding disclosure of CPNI by wireless users in *United States West, Inc. v. FCC*[306]

As federal telecommunications laws now stand, 47 U.S.C. § 222 governs the privacy of cellular telephone customer information. The statute places a duty on telecommunications carriers to protect the confidentiality of customer information:

> A telecommunications carrier that receives or obtains [CPNI} proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.[307]

With regard to wireless location information, 47 U.S.C. § 222(f) requires "express prior authorization of the customer" before "use or disclosure of or access to-- (1) call location information concerning the user of a commercial mobile service"[308] other than in accordance with emergency notification services as provided under 47 U.S.C. § 222(d)(4). Under 47 U.S.C. § 222(h)(1) customer proprietary network information (CPNI) includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[309]

However, under 47 U.S.C. § 222(c)(3) "[a] telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information" for purposes other than provision of telecommunications service or services necessary to the provision of such service.[310] "Aggregate information" is defined in 47 U.S.C. § 222(h)(2) as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[311] As a result of this complex legislation, location information is routinely collected by wireless telecommunications providers. Access to this information depends on the nature of the user, the consent of the wireless subscriber and the purposes for which the location information is used.

The recently adopted FCC order allocating bandwidth for Dedicated Short Range Communications in ITS Applications, discussed above,[312] is intended to facilitate inclusion of wireless radio communications devices in new vehicles (OBUs) and installation of communications nodes along roadsides (RSUs). One could

---

[304] 47 U.S.C. § 222(a).

[305] *Id.* § 222(c).

[306] 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000) (vacating on First Amendment grounds a FCC order restricting wireless carriers from using and disclosing CPNI).

[307] 47 U.S.C. § 222(b).

[308] *Id.* § 222(f).

[309] *Id.* § 222(h)(1).

[310] *Id.* § 222(c)(3).

[311] *Id.* § 222(h)(2).

[312] *See* discussion *supra* note 59.

argue that, since these OBUs are wireless telecommunications devices, that information from them should be treated in the same way as location information from wireless telephones which is protected as CPNI. However, the new ITS Rule and Order, noted above, says nothing about protecting the privacy of DSRC users. As a practical matter, some of the DSRC technology, particularly the geographically limited stand-alone roadside units, might not be treated as interstate telecommunications carriers under federal law and, as a result, not CPNI. In short, considerable uncertainty remains about the privacy of the new ITS communications applications.

State Legislation

In contrast with the generally permissive federal laws regarding privacy on roadways, state statutes designed to protect privacy on the open road tend to offer more privacy protection, although there is considerable variation. For example, the state statutes regulating electronic tracking devices discussed above[313] offer considerably more protection for roadway privacy than applicable federal statutes.

Several states have enacted legislation restricting photo radar and red light cameras described above.[314] One of the first such statutes was enacted by New Jersey in 1992.[315] The prohibition is direct and unequivocal: "Notwithstanding any law, rule or regulation to the contrary, a law enforcement officer or agency shall not use photo radar to enforce the provisions of [traffic regulations] . . . ."[316] The Utah statute's prohibition on photo radar is subject to exceptions, such as allowing use of photo radar in school zones. The Utah statute also requires posting of warning signs and requires local option before radar is used.[317] The Oregon statute only authorizes photo radar in seven specified municipalities which can decide whether or not to use photo radar. The Oregon statute also requires signs warning of the use of photo radar, limited hours of use and a number of other restrictions.[318] Nevertheless, photo radar remains widely used in the United States, aside from the states where these statutory restrictions apply.

Other state statutes address misuse of remote cameras. A California statute has recently authorized an action for "constructive invasion of privacy" under California Civil Code section 1708.8(b):

> A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording , or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.[319]

Using electronic devices to capture images of personal or family activities is grounds for civil liability in California, even when there is no physical trespass on the property of the victim. Misuse of remote cameras to

---

[313] *See* discussion *supra* notes 200-03.

[314] Five states appear to have statutes that specifically address the use of photo radar: California, New Jersey, Utah, Wisconsin, and Oregon.

[315] N.J. STAT. ANN. § 39:4-103.1 (West 2002). California and Wisconsin also prohibit use of photo radar in speed enforcement. CAL. VEH. CODE § 21455.6(c) (West 2000); WIS. STAT. ANN. § 349.02(3)(b) (West 2000).

[316] N.J. STAT. ANN. § 39:4-103.1(a).

[317] UTAH CODE ANN. § 41-6-52.5 (1998).

[318] OR. REV. STAT. § 810.438 (2003).

[319] CAL. CIV. CODE § 1708.8(b) (West Supp. 2004).

probe the interiors of apartments along the highway would appear to violate this statute. Since the concept of constructive invasion of privacy protects all areas where one has "a reasonable expectation of privacy," such areas could potentially include the interiors of vehicles, particularly mobile homes, on the open road.

The most recent, and in many ways the most interesting, example of state legislative restrictions on roadway surveillance technology is what is called "black box" legislation restricting the availability of information from the computer diagnostic modules described, supra.[320] A recently enacted California Statute, Vehicle Code section 9951 provides that 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),' shall disclosure that fact in the owner's manual."[321] The statute covers devices that record such factors as the vehicle's speed and direction, the history of where the vehicle has traveled, vehicle steering performance, use and performance of breaks, or the driver's use (or not) of a seatbelt. It also covers any device that has the capacity to transmit information about an accident in which the vehicle has been involved to a central receiving system when an accident occurs.[322] Such "black box" information is routinely downloaded by insurance companies and vehicle manufacturers for use in determining the causes of and liability for accidents.

The statute also restricts data derived from such devices. "Black box" data cannot legally be downloaded or otherwise retrieved by anyone other than the registered owner of the vehicle, except with the consent of the vehicle owner. However, the data can be produced in response to a lawful court order. It can also lawfully be used for motor vehicle safety research, provided that the identity of the registered owner or driver are not disclosed. Automotive technicians are permitted access to "black box" for the purposes of servicing or repairing the vehicle, but are restricted from releasing the data. The statute also specifically requires that telematics subscription services (such as OnStar, discussed above) disclose their capacity to record or transmit vehicle diagnostic information as part of their subscription services.

So far, California is the only state to establish that a vehicle owner or driver is the owner of vehicle diagnostic information. To the extent that this data-ownership model is extended to other types of information derived from the activities of people on the open road, protection for the privacy interests of roadway users will be further reinforced.

V. Conclusion

The principle that people on the open road have the right to control information about their on-the-road activities underlies the recent California Statute regarding onboard black box diagnostic units just discussed. Such a principle also contributes to many of the other types of privacy rights discussed in this article. Returning control over information about the activities of people on public roads and highways to the individuals who are the subjects of that information is an appropriate and effective strategy for protecting autonomy and information privacy interests of people on the open road.

Respect for the individual person and insistence on each person's rights to dignity and self-determination underlie the laws that protect the privacy of people on public roads and highways. These laws protect both autonomy privacy rights concerned with where an individual can freely choose to go and also information privacy rights to control collection and disclosure of information collected about the individual's whereabouts.

A half-century ago, Justice William O. Douglas described privacy interests as radiating out from the individual in concentric circles:

> First is the autonomous control over the development and expression of one's intellect, interests, tastes,

---

[320] *See* discussion *supra* notes 45-49.

[321] CAL. VEH. CODE § 9951(a) (West Supp. 2004).

[322] *Id.* § 9951(b).

and personality.

. . . .

Second is freedom of choice in the basic decisions of one's life respecting marriage, divorce, procreation, contraception, and the education and upbringing of children.

. . . .

Third is the freedom to care for one's health and person, freedom from bodily restraint or compulsion, freedom to walk, stroll, or loaf.[323]

It is to this outer edge of privacy interests, that this article has directed attention.

Out there on the open road, important privacy interests are worthy of recognition and protection. Examining these outlying privacy interests in light of advances in technologies designed to continuously keep track of everyone's whereabouts spotlights some of the privacy rights that have been out there on the open road all along, perhaps unseen and unappreciated.

[323] Doe v. Bolton, 410 U.S. 179, 211-13 (1973) (Douglas, J., concurring) (emphasis omitted).