Richmond Journal of Law and Technology

Volume 18 | Issue 1 Article 2

2011

Current and Emerging Transportation Technology: Final Nails in the Coffin of the Dying Right of Privacy?

James D. Phillips
University of Richmond

Katharine E. Kohm

CURRENT AND EMERGING TRANSPORTATION TECHNOLOGY: FINAL NAILS IN THE COFFIN OF THE DYING RIGHT OF PRIVACY?

By James D. Phillips* & Katharine E. Kohm**

Cite as: James D. Phillips & Katharine E. Kohm, *Current and Emerging Transporation Technology: Final Nails in the Coffin of the Dying Right of Privacy,* XVIII RICH. J.L. & TECH. 1, http://jolt.richmond.edu/v18i1/article1.pdf

I. INTRODUCTION

[1] Transportation networks constitute "the circulatory system of our economy."[1] The distinct modes that constitute the American

* B.A. Government and Foreign Affairs, Hampden-Sydney College, J.D. University of Richmond School of Law, Ph.D., Public Administration, University of Colorado. Dr. Phillips is a former Assistant Attorney General of Virginia and General Counsel to the Virginia Department of Transportation. He is an Adjunct Professor of Law at the University of Richmond School of Law, Visiting Scholar at George Washington University in Washington, D.C., and the Director of the Conflict Resolution Institute in Richmond, Va.

** B.S. Civil Engineering, University of Virginia, J.D., University of Richmond School of Law. Ms. Kohm is an associate at Little, Medeiros, Kinder, Bulman & Whitney, P.C. in Providence, R.I., where her practice focuses primarily on business litigation and construction law. Prior to entering private practice, Ms. Kohm clerked for the Honorable Justice Gilbert V. Indeglia of the Rhode Island Supreme Court.

transportation system—air, rail, transit, highways, and waterways—impact the entire range of our daily activities.[2] Just as the human body depends on its circulatory system for life and well being, the United States' vitality would grind to a halting stop without a vibrant transportation system.

[2] Ongoing globalization, population growth, and urbanization continue to overload transportation systems in this country and around the world.[3] As a result, our transportation system relies on advancing technology and its applications to sustain its operation in response to modern demands.[4] However, an unintended consequence of this increased reliance on technology is the widespread collection of vehicular, personal, and company data for the delivery of services.[5] Consequently, concerns exist as to whether all of the personal data being collected is actually necessary, whether it contains sensitive personal information,

† The authors would like to thank Ray D. Pethtel, Transportation Fellow and Interim Executive Director of the I-81 Coalition, and Gene Hetherington, Doctoral Candidate and Graduate Assistant at the Virginia Tech Transportation Institute in Blacksburg, Va. for their generous assistance with this article. This article grew out of our research for the previously published Policy Paper, "A Policy Review of the Impact of Existing Privacy Principles have on Current and Emerging Transportation Safety Technology".

[1] IBM CORP., THE CASE FOR SMARTER TRANSPORTATION 2 (2010) [hereinafter IBM, SMARTER TRANSPORTATION], *available at* http://www-07.ibm.com/innovation/my /exhibit/documents/pdf/2_The_ Case_For_Smarter_Transportation.pdf.

[2] *Id.*

[3] *Id.*

[4] *See id.* at 5 (discussing the importance of digital technology to "model future demand, capacity, cost and impacts").

[5] *See* Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 296 (2004).

such as bank account and Social Security numbers, and whether it is managed to safeguard personal privacy.[6]

[3] Advancing technologies have increased the transportation system's capacities, but have also provided more opportunities and methods to invade an individual's privacy interests.[7] The escalating issue of personal privacy threats caused by transportation technologies has raised questions as to how to protect a traveler's privacy interests, if the interests deserve protection at all.[8] In 2009, Missouri state senator Jim Lembke introduced a bill to ban the increasing use of red light cameras.[9] He argued: "We've got a real problem with these red light cameras and how they infringe upon our constitutional rights. Rights to privacy, rights to equal protection under the law, rights to do [sic] process and the right to confront our accuser."[10]

---

[6] *See* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1387 (2004) (discussing how new highway technologies can provide "invaluable information on traffic, weather, and road conditions," but can also, in many cases, collect personal information about the "movements and driving habits of particular drivers"); *see also* Benjamin Burnham, Comment, *Hitching a Ride: Every Time You Take a Drive, the Government Is Riding with You*, 39 J. MARSHALL L. REV. 1499, 1513 (2006) (discussing how personal data collected through electronic tollway systems, such as E-ZPass, have been subpoenaed by private lawyers in divorce cases).

[7] *See* Glancy, *supra* note 5, at 296.

[8] *See* Frank Douma & Jordan Deckenbach, *The Challenge of ITS for the Law of Privacy*, 2009 U. ILL. J.L. TECH. & POL'Y 295, 328.

[9] Joel O. Christensen, Note, *Wrong on Red: The Constitutional Case Against Red-Light Cameras*, 32 WASH. U. J.L. & POL'Y 443, 460-61 (2010) (discussing the presence of legal concerns about red lights in Missouri since 2006); Press Release, Mo. Senate, Senator Jim Lembke Introduces His First Bills in Mo. Senate (Jan. 21, 2009), *available at* http://www.senate.mo.gov/09info/members/newsrel/d01/012109.pdf.

[10] *Outlawing Red Light Cameras Proposed in Senate Committee* (NewsRadio 1120 KMOX News radio broadcast Feb. 18, 2009) (transcript on file with Missouri Digital

[4] Historically, the American people have held personal privacy as a sacred value, a result of either our historical roots as British colonies or our rugged individualism.[11] For whatever reason, the United States has a long-standing perception that the protection of personal sensitive information is an absolute right of citizenship.[12] That is, of course, not the case. There is no specific constitutional right to privacy, but there are numerous case decisions and individual statutes that bear on the question of whether, and to what extent, a citizen's expectation of privacy exists.[13] This article will elaborate on the question of whether a member of the traveling public carries a legally protected privacy right in the transportation arena.

[5] As this article already pointed out, a vibrant transportation system is fundamental to the commercial operations, the security, and the overall health and vitality of the United States and its society.[14] In recent years,

---

News), *available at* http://mdn.org/2009/stories/redlight.htm.

[11] *See* James M. Rosenbaum, *In Defense of the Hard Drive*, 4 GREEN BAG 2D 169, 170 (2001) ("In the years leading to the Revolutionary War, the British used general searches as a way to root out anti-English traitors and sympathizers. The citizens of the nascent Republic found these searches wholly unreasonable."); Amanda Christine Dake, Comment, *The Application of "Out-of-Hospital" Do not Resuscitate Order Legislation to Commercial Airline Travel*, 63 J. AIR L. & COM. 443, 455-56 (1997) ("[B]ecause historically Americans have understood personal privacy to involve a 'right to be let alone,' the right of privacy exemplifies basic tenets of 'the American way of life' and vision of liberalism, or, rather, dedication to individualism, the rule of law, and freedom from unwarranted governmental intrusions into individuals' private affairs.") (quoting DAVID M. O'BRIEN, THE RIGHT OF PRIVACY– ITS CONSTITUTIONAL & SOCIAL DIMENSIONS: A COMPREHENSIVE BIBLIOGRAPHY, at ii (1980)).

[12] *See* DAVID SADOFSKY, THE QUESTION OF PRIVACY IN PUBLIC POLICY: AN ANALYSIS OF THE REAGAN-BUSH ERA 1 (1993) ("Three out of four Americans were discovered to believe the 'right of privacy' should be akin to the inalienable rights to life, liberty and the pursuit of happiness, the traditional promises of the Declaration of Independence.").

[13] *See, e.g.*, Roe v. Wade, 410 U.S. 113, 152 (1973) (citing various Supreme Court decisions that recognized a right to privacy under the Constitution).

[14] *See* IBM, SMARTER TRANSPORTATION, *supra* note 1, at 2.

the development of transportation-related technologies has become the focus of more and more business operations, and with that the issue of the legal protection of individual privacy in the face of these technological developments has earned increased scrutiny.[15] Moreover, in the post 9/11 era, the issue of national security has focused primarily on specific transportation modes: air, rail and highways.[16] This has placed greater emphasis on national security which has, at times, collided with the protection of an individual's privacy interests while traveling.[17] This article examines the impact that advancing transportation technology has on the traveling public's expectation of privacy, as well as how the United States Supreme Court, the Congress, the courts in Virginia and the General Assembly of Virginia have addressed privacy claims in a host of situations. These statutory requirements and judicial opinions will be discussed and analyzed, concluding that a critical outcome of emerging transportation technology has been the narrowing and eroding of the scope of legally protected privacy interests.

---

[15] *See* Blitz, *supra* note 6, at 1387; Douma & Deckenbach, *supra* note 8, at 296; *see also* Burnham, *supra* note 6, at 1499.

[16] *See* Kyle P. Hanson, Note, *Suspicionless Terrorism Checkpoints Since 9/11: Searching for Uniformity*, 56 DRAKE L. REV. 171, 172-75 (2007). *See generally* John W. Whitehead & Steven H. Aden, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives*, 51 AM. U. L. REV. 1081, 1108 (2002) (examining the USA Patriot Act's effect on private protections).

[17] *See* Hanson, *supra* note 16, at 172-75 (providing examples of instances where travelers are subjected to "suspicionless searches").

II. THE LEGAL LANDSCAPE

A. United States Supreme Court Decisions

[6] Neither the U.S. Constitution, nor the Bill of Rights, contains explicit provisions for the protection of privacy.[18] However, the Supreme Court of the United States in *Griswold v. Connecticut* famously recognized that "specific guarantees in the *Bill of Rights* have penumbras" that "create zones of privacy."[19] The *Griswold* Court noted that "facets of privacy" appear within the First Amendment's right of association, the Third Amendment's "prohibition against the quartering of soldiers 'in any house,'" the Fourth Amendment's protection from unreasonable government search and seizure, and the Fifth Amendment's protection from self incrimination that "enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment."[20] The Court explained that, when reading these penumbrae together with the Ninth Amendment's assurance that "[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others," the Constitution arguably reserves a tacit right of privacy.[21] After *Griswold* and the Supreme Court's ostensible nod in the direction of accepting a general right to privacy, the Court seemingly has limited its *Griswold* pronouncement to zones of privacy concerning familial and personal relationships, rather than expanding the right to an individual's control of information dissemination.[22] Contributing further questions and

[18] *Roe*, 410 U.S. at 172.

[19] Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (concluding that a state statute criminalizing contraceptive use by married couples intruded into a zone of marital privacy where the government may not tread).

[20] *Id.* at 484.

[21] *Id.* (quoting U.S. CONST. amend. IX).

[22] Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643, 644 (2007) ("[T]he controversy over reproductive privacy decisions makes expansion of [informational] privacy protections unlikely for the foreseeable future. This

contradictions, constitutional scholars also disagree whether privacy actually is a valid legal concept.[23]

[7] For example, in *Katz v. United States*, the Court ruled that the use of electronic surveillance in a public telephone booth without a search warrant violated the Fourth Amendment's protection against unreasonable search and seizure and affirmed that the Fourth Amendment's protection extends to public places.[24] The Court later noted in *United States v. Miller* that individuals had no expectation of privacy for information supplied voluntarily for commercial uses.[25] Thereafter, in *Whalen v. Roe*, the Court attempted to define a balance between the interests of privacy and the government's operations.[26] In *Whalen*, the Court ruled that New York State had the right to collect data about individuals and create a database if for the public good and with adequate security measures taken to protect the privacy and identification of individuals.[27] As part of this ruling, the Court recognized and defined what it called a "zone of privacy" in which an individual may have the expectation of the nondisclosure of personal

is unfortunate, and even tragic, because technology for learning and disseminating highly personal things about individuals poses an unprecedented risk of invasion of privacy.").

[23] *Compare* ROBERT H. BORK, THE TEMPTING OF AMERICA: THE POLITICAL SEDUCTION OF THE LAW 95-96, 199-206, 210-13 (1990) ("Related to . . . Tribe's discussion of rights of privacy and personhood . . . are rights of individual autonomy which inhere in the Constitution because that document is claimed to have an implicit idea of what it means to be fully human. Quite aside from the dubious nature of that assertion, Tribe's version of what being human is turns out to be an extreme form of modern liberalism's moral relativism."), *with* LAURENCE H. TRIBE, CONSTITUTIONAL CHOICES 12-13 (1985) ("A substantive concern for individual privacy necessarily underpins the Fourth Amendment.").

[24] *See* Katz v. United States, 389 U.S. 347, 358-59 (1967).

[25] *See* United States v. Miller, 425 U.S. 435, 442-43 (1976).

[26] *See* Whalen v. Roe, 429 U.S. 589, 591-95, 600-02 (1977).

[27] *See id.* at 605-06.

matters and "independence in making certain kinds of important decisions."[28]

[8] Relative to transportation privacy, the Court in *Delaware v. Prouse* agreed that without "at least [an] articulable and reasonable suspicion that a motorist is unlicensed or that an automobile is not registered, or that either the vehicle or an occupant is otherwise subject to seizure for violation of law," law enforcement could not randomly stop vehicles to check for valid license and registration.[29] The Court articulated that "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."[30] Nonetheless, the *Prouse* Court curtailed broad privacy protections for individual drivers when it recognized that, even without probable cause or reasonable suspicion, constitutionally acceptable methods for stopping vehicles exist.[31] As long as police officers do not have "the unbridled discretion" to stop any random vehicle, instead maintaining a systemic "[q]uestioning of all oncoming traffic at roadblock-type stops," then such stops pass constitutional muster.[32]

[9] A mere four years following the *Prouse* decision, the Court reigned in privacy protections again when it found that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[33] In *United States v. Knotts*, the police put a tracking device on a container of

[28] *Id.* at 598-600.

[29] Delaware v. Prouse, 440 U.S. 648, 663 (1979).

[30] *Id.* at 662.

[31] *See id.* at 663.

[32] *Id.*

[33] United States v. Knotts, 460 U.S. 276, 281 (1983).

chemicals picked up and transported in a car without first obtaining a warrant.[34] Following the tracking device signal to a secluded cabin in the woods, the police conducted visual surveillance for three days before obtaining a search warrant for the cabin.[35] The Court took no exception to the police's tactics and found that the "beeper signals complained of by respondent [did not] invade any legitimate expectation of privacy," and thus "there was neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment."[36] In response to respondent's argument and warning that holding in the government's favor may mean that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision,"[37] the Court commented that it has "never equated police efficiency with unconstitutionality."[38] Given the compendium of the *Prouse* and *Knotts* holdings, it almost goes without mention that the High Court has established a generally accepted maxim that persons traveling in vehicles on public highways have significantly diminished expectation of any right to privacy.[39]

[10] These Supreme Court decisions painted the backdrop for individual privacy protections leading up to the technological explosion, and created, at best, a muddled legal standard for privacy.[40] This issue

[34] *Id.* at 278-79.

[35] *Id.*

[36] *Id.* at 285.

[37] *Id*. at 283.

[38] *Knotts*, 460 U.S. at 284.

[39] *See* Robert H. Whorf, *"Coercive Ambiguity" in the Routine Traffic Stop Turned Consent Search*, 30 SUFFOLK U. L. REV. 379, 397 (1997) ("The United States Supreme Court's greatly diminished view of Fourth Amendment privacy protection for motorists on public roadways is not in accord with the reality of citizens' use and view of their cars.").

[40] Chemerinsky, *supra* note 22, at 656 (discussing the "unprecedented access to information about individuals," and the serious need for "judicial protection of a

became even more complex with the development of emerging technologies—such as camera-based applications, satellite communications and tracking, electronic databases, and the Internet—that facilitate the collection and storage of personal information.[41] Moreover, in the post 9/11 era, the threats to national security by terrorist groups and others have led to a heightened emphasis on homeland security.[42] This focus on security has further eroded already uncertain legal protections for an individual's expectation of privacy in his/her personal data.[43] While the Supreme Court has addressed several cases arising from privacy protection challenges to technological innovation,[44] the development of the law in the transportation arena has occurred primarily by congressional enactments and the regulatory framework.[45]

---

constitutional right to informational privacy and greater safeguards through tort law and statutes").

[41] *See id.* ("Computerized records and databases store information in a way that it can be accessed by others. The Internet makes it potentially available to many.").

[42] *See* Patrick E. Tolan, Jr., *Homeland Security Challenges of Global Climate Change*, 54 LOY. L. REV. 800, 812 (2008) ("To say 'the world has changed after 9/11,' is an understatement, especially regarding the importance of making the proper access decisions. Indeed, national awakening to this threat after 9/11 is what prompted the placement of [Citizenship and Immigration Services ("CIS")] within the Department of Homeland Security in the first place.").

[43] *See, e.g.*, Whitehead & Aden, *supra* note 16, at 1108 (examining the USA Patriot Act's effect on privacy protections and noting that requests to install wiretaps to record private conversations now are "virtually never denied").

[44] *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010) (upholding privacy expectations in communications made on electronic equipment owned by a government employer); *Reno v. Condon*, 528 U.S. 141 (2000) (finding that the South Carolina department of motor vehicles' requirement that automobile owners provide personal information as a condition of obtaining a driver's license or registering a vehicle, and the selling of this personal data for revenue, are in conflict with Driver's Privacy Protection Act of 1994).

[45] *See* Douma & Deckenbach, *supra* note 8, at 305 ("Although there is not a single comprehensive privacy statute or constitutional provision in the United States, statutes have been passed to address specific privacy concerns. In many cases, these have

B. Federal and State Statutes and Regulations

[11] Whether there is a causal relationship between the events of 9/11 and the "explosion" of technology in the security arena is an important analysis that is beyond the scope of this research. However, it is incontrovertible that efforts to improve the technologies attendant to data security, especially in the transportation arena, have given rise to increasing concern for privacy protection.[46] The development of now commonplace technologies such as sophisticated electronics, computers, and the wireless Internet have provided capabilities that previous generations could only dream of and many in our current society can barely comprehend.[47] Whether due to the fear of the unknown or the understanding of the known, technological advancements have triggered citizen concern and Congress has responded with a series of enactments which, in turn, have resulted in regulatory promulgations.[48] While an exhaustive discussion of congressional action would prove formidable, the following is an overview of the landscape.

[12] Title 6 of the United States Code, Domestic Security, establishes the Department of Homeland Security.[49] Chapter 4 of Title 6 provides the statutory framework for transportation security including: surface

stemmed from public outcry over a revealed gap in privacy laws; accordingly, they address only those specific instances of privacy concerns.").

[46] *See generally id.* at 305-06, 308-10, 326.

[47] *Cf.* Robin Cowan, *High Technology and the Economics of Standardization*, U. W. ONTARIO, 12 (May 27-28, 1991), http://www.cgl.uwaterloo.ca/~racowan/High TechStand.pdf (presented at the International Conference on Social and Institutional Factors Shaping Technological Development: Technology at the Outset) ("It may be . . . very difficult to predict what properties [technologies] will have in the future.").

[48] *See generally* Douma & Deckenbach, *supra* note 8, at 305 (citing as an example the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (2006)).

[49] 6 U.S.C. § 111.

transportation security,[50] railroad security,[51] and over-the-road-bus and trucking security.[52] In each of these areas, Congress has mandated that the Secretary of Homeland Security identify risks and areas of vulnerability, as well as promote research into tactics and strategies for mitigating the risks and addressing emergency situations should they occur.[53]

[13] Of particular relevance to this discussion is the language in Title 6, wherein Congress authorized the Secretary of Homeland Security to permit "deploying, equipping, and utilizing tracking technology . . . for motor carriers transporting security-sensitive materials" in order to collect, display, and store information regarding the movements and locations of shipments and vehicles.[54] Moreover, this section enables the "installation by a motor carrier of concealed electronic devices . . . activated by law enforcement authorities to disable the vehicle or alert emergency response resources to locate and recover security-sensitive materials . . . ."[55]

[14] Included in Title 49 of the United States Code is a provision that "the Secretary of Homeland Security shall develop, prepare, implement and update . . . (A) National Strategy for Transportation Security; and (B) transportation modal security plans" addressing security risks including threats, vulnerabilities, and consequences for "aviation, bridge and tunnel, commuter rail and ferry, highway, maritime, pipeline, rail, mass transit,

[50] *See* 6 U.S.C. §§ 1151-1208 (Supp. III 2010).

[51] *See id.* §§ 1161-1172.

[52] *See id.* §§ 1181-1186.

[53] *See id.* §§ 1101-1186.

[54] *Id.* § 1204(a)(2)(C)(i) (Supp. III 2010).

[55] 6 U.S.C. § 1204(a)(2)(C)(v) (Supp. III 2010). This type of legislation—according to those advocates who fear the misuse and abuse of secretly tracking motor vehicles for any purposes—further erodes the right to privacy for all members of the traveling public. *See* Glancy, *supra* note 5, at 295-96. The discussion will return to motor vehicle tracking by law enforcement officials in Part III.

over-the-road bus, and other public transportation infrastructure assets."[56] The statute further provides that the Secretary of Homeland Security and the Transportation Secretary shall work jointly to develop, revise and update the National Security Strategy by identifying "transportation assets in the United States that . . . must be protected from attack or disruption by terrorists or other hostile forces . . . ."[57]

[15] In the area of motor vehicles, traditionally a state law jurisdiction, the Driver's Privacy Protection Act of 1994 (DPPA) prohibits the release and use of certain personal information from state motor vehicle records.[58] The statute prohibits the state motor vehicles department from disclosing personal information, including photographs, social security numbers, and any personally identifying data to any entity or person without the consent of the individual to whom the information applies.[59] Congress did create an exception, however, in cases where personal information is sought for such reasons as "motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories," or law enforcement purposes.[60]

[16] Dorothy Glancy, in her seminal discussion of privacy issues encountered by citizens on America's highways, concluded with a review of a California statute that mandates automobile manufacturers to disclose the presence of event data recorder (EDR) mechanisms in the owner's manuals of new automobiles manufactured after July 1, 2004, and sold or leased in the state of California.[61] These EDR "black boxes" have the

[56] 49 U.S.C. § 114(s)(1)(A)-(B) (Supp. III 2010).

[57] *Id.* § 114(t)(3)(A).

[58] 18 U.S.C. § 2721 (2006).

[59] *Id.* §§ 2721, 2725(4).

[60] *Id.* § 2721(b)(1); *see also* Reno v. Condon, 528 U.S. 141, 145 (2000).

[61] Glancy, *supra* note 5, at 374 (citing CAL. VEH. CODE § 9951 (Deering, LEXIS through 2011 Sess.)).

capacity to collect and record information from the vehicle such as speed, direction, travel history, seatbelt use by the driver, and accident-related data.[62] The statute further requires that data may only be released with the consent of the owner for certain types of research about safety issues, or in response to a lawful court order. [63] Glancy hypothesized that, given the California statute's level of privacy protection for EDR data, when "other types of information derived from the activities of people on the open road [is collected], protection for the privacy interests of roadway users will be further reinforced."[64]

[17] Since 2004, twelve other states have enacted a statute similar to California's "black box" legislation, which indicates that Glancy's hypothesis was, at least in part, accurate.[65] As with the California statute, these twelve state statutes require the owner's consent prior to releasing data.[66] Exceptions include: (1) release pursuant to a valid court order or search warrant; (2) release for research purposes; or (3) release for diagnostic purposes, such as servicing or repairing the motor vehicle.[67]

---

[62] *Id.*

[63] *Id*. at 375.

[64] *Id.*

[65] *See* ARK. CODE ANN. § 23-112-107 (2011); COLO. REV. STAT. § 12-6-402 (2010); CONN. GEN. STAT. § 14-164aa (Supp. 2011); ME. REV. STAT. ANN. tit. 29-A, §§ 1972-1973 (2011); NEV. REV. STAT. ANN. § 484D.485 (Lexis-Nexis 2011); N.H. REV. STAT. ANN. § 357-G:1 (LexisNexis 2011); N.Y. VEH. & TRAF. LAW § 416-b (Consol. Supp. 2011); N.D. CENT. CODE § 51-07-28 (2011); OR. REV. STAT. §§ 105.928, .932, .935, .938, .942, .945 (2009); TEX. TRANSP. CODE ANN. § 547.615 (West 2011); VA. CODE ANN. § 46.2-1088.6 (West Supp. 2011); WASH. REV. CODE ANN. §§ 46.35.020, 0.30 (Supp. 2011).

[66] *See* sources cited *supra* note 65.

[67] *See, e.g.*, NEV. REV. STAT. ANN. § 484D.485(2); N.D. CENT. CODE. § 51-07-28(2); TEX. TRANSP. CODE ANN. § 547.615(c); VA. CODE ANN. § 46.2-1088.6; WASH. REV. CODE ANN. § 46.35.030(1)(a)-(c).

[18] The owner's consent requirement receives additional bolstering in Oregon and North Dakota, where state statutes prohibit insurers from requiring the insured to provide automatic consent for the insurer to retrieve EDR data as a condition of obtaining an insurance policy.[68] Notably, the data can be released without the owner's consent if "[a] law enforcement officer, firefighter or emergency medical services provider seeks to obtain the data in the course of responding to or investigating an emergency involving the physical injury or the risk of physical injury to any person."[69] Maine and Washington have similar exceptions for releasing vehicle data in the event of medical emergencies in order to treat injured individuals.[70]

[19] A discussion of the California and other twelve state statutes sets the background for a discussion of other federal regulations in this area.[71] The Code of Federal Regulations, Title 49, §§ 563.1 through 563.12, establishes "national requirements for vehicles equipped with event data recorders (EDRs) concerning the collection, storage, and retrievability of onboard motor vehicle crash event data" for vehicles manufactured after September 1, 2012.[72] Rather than protecting driver privacy, the primary purposes of these regulations are: (1) addressing safety concerns; (2) advancing the understanding of accident causation; and (3) developing safer vehicle designs.[73] Section 563.11 does mandate disclosure of the EDR device in the owner's manual, but none of the regulatory sections

[68] N.D. CENT. CODE § 51-07-28(6); OR. REV. STAT. § 105.932.

[69] OR. REV. STAT. § 105.935.

[70] ME. REV. STAT. ANN. tit. 29-A, § 1972; WASH. REV. CODE ANN. § 46.35.030(1)(d).

[71] *See generally supra* text accompanying notes 61–67 (discussing the hypothesis that California and other states' "black box" legislation will enhance driver's information privacy and autonomy).

[72] 49 C.F.R. §§ 563.1, 563.3 (2010).

[73] *See id*. § 563.2.

specifically require the owner's consent to release data after an accident.[74] Although no personal data, such as name, gender, age or accident location is recorded or released by the EDR, federal regulations explicitly acknowledge that law enforcement officials have access to this personal information in accident investigations, which could be combined with EDR data without an owner's consent.[75]

[20] The Federal Trade Commission (FTC) Act of 1914 granted the agency the power to prevent unfair business practices,[76] which now includes the Principles of Fair Information Practices, governing information over the Internet.[77] The FTC describes Congress' approach to addressing privacy concerns as "'sectoral,' consisting of a handful of disparate statutes" that address "different commercial activities [with] different privacy issues."[78] Once the FTC realized the privacy concerns

[74] *See id*. § 563.11.

[75] *See id.*

[76] *See* Federal Trade Commissions Act, 15 U.S.C. §§ 41, 58 (2006).

[77] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS, 7-8 (June 1998), http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[78] Christine A. Varney, Comm'r, Fed. Trade Comm'n, Remarks at the Privacy & American Business National Conference: Consumer Privacy in the Information Age: A View From the United States (Oct. 9, 1996); *see* Ray D. Pethtel, James D. Phillips & Gene Hetherington, *A Policy Review of the Impact Existing Privacy Principles Have on Current and Emerging Transportation Safety Technology*, THE NAT'L SURFACE TRANSP. SAFETY CTR. FOR EXCELLENCE, 9 (May 12, 2011), http://scholar.vt.edu/VTTI/reports/PrivacyFinalReport05122011.pdf ("In 1998, Congress recognized that the privacy protections provided by the FTC were inadequate, describing the situation as 'sectoral,' consisting of a handful of disparate statutes directed at specific industries that collect personal data and none of which specifically cover the general collection of personal information."); *see, e.g.*, Right to Financial Privacy Act of 1978, 12 U.S.C. § 3402 (2006) (governing individual bank records); Fair Credit Reporting Act, 15 U.S.C. § 1681c(a) (2006) (governing consumer credit reports); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511 (2006 & Supp. II 2010) (governing the disclosure of wire, oral, or electronic communications); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2006) (governing video rental records); Family Educational Rights and

inherent in such a fractured system they created the Principles of Fair Information Practices, attempting to encourage the private sector to create and utilize a system of self-regulation.[79] The uncertainty involved with interpreting each of these statutes to find a common set of privacy standards has "conspired to create an environment where any regulation of privacy is not only open to an endless number of interpretations but also creates a liability minefield for companies that develop, manufacture and deploy technology that involves the collection of private information."[80] Perhaps with the mandate from the Principles of Fair Information Practices, the private sector and non-governmental organizations (NGOs) will "fill the void by creating regulatory systems designed to … protect their institutional interests."[81]

Privacy Act of 1974, 20 U.S.C. § 1232g (2006) (governing student records); Communications Act of 1934, 47 U.S.C. § 151 (1934) (current version at Telecommunications Act of 1996, 47 U.S.C. § 222 (2006)) (governing information relating to use of telecommunication services; "customer proprietary network information"); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2006) (governing cable television subscriber information); *cf.* Privacy Act of 1974, 5 U.S.C. § 552a (2006) (governing data collected by the federal government). Pursuant to the Supreme Court's decision in United States v. Miller, 425 U.S. 435 (1976), individuals have no Fourth Amendment interest in personal information they voluntarily have conveyed to another. Consequently, any privacy protections for personal information must be legislatively grounded.

[79] Pethtel, Phillips & Hetherington, *supra* note 78, at 9; *see* FED. TRADE COMM'N, *supra* note 77, at 15-16.

[80] Pethtel, Phillips & Hetherington, *supra* note 78, at 9; *see, e.g.*, Rebecca Dent, *The Role of Banking Regulations in Data Theft and* Security, 27 REV. BANKING & FIN. L. 381, 390 (2008) ("Illinois's Credit Card and Debit Card Liability Act would amend current Illinois identity theft legislation to make any data collector, such as TJX, liable to any financial institution for costs associated with identity theft originating with the data collector.").

[81] Pethtel, Phillips & Hetherington, *supra* note 78, at 9-10; *see* FED. TRADE COMM'N, *supra* note 77, at 15 (illustrating how the "online industry" has used self-regulation to effectively protect online privacy).

[21] One example of such an effort was undertaken by a group of transportation equipment manufacturers who are members of the Intelligent Transportation Society of America (ITSA).[82] Established in 1991, ITSA is a public/private partnership dedicated to promoting the development and deployment of variety of intelligent transportation technologies.[83] ITSA creates technology devices that apply to almost all areas of the transportation sector.[84] In response to an increased concern over data security, the ITSA created a task force charged with studying the issue and offering recommendations that would address the public concerns about how emerging transportation technology should be regulated to best protect the public's privacy interests.[85] After approval from the ITSA's Board, the principles were created as non-binding guidelines and member organizations were not compelled to comply with the principles, but merely to agree to take them into account in the development process of any new technology.[86] These Privacy Principles

[82] *See* Pethtel, Phillips & Hetherington, *supra* note 78, at 1; *Membership,* ITS AM., http://www.itsa.org/membership (last updated July. 13, 2011).

[83] *See About ITS America*, ITS AM., http://www.itsa.org/aboutus (last updated June 24, 2011).

[84] *See* Pethtel, *supra* note 78, at 23 (providing multiple examples of technologies created by ITSA members); *Connected Vehicle Insights: Trends in Machine-to-Machine Communications*, ITS AM., 2-6 (2011), http://www.itsa.org/knowledgecenter/technologyscan (under "Current Connected Vehicle Insight Reports* under production," follow either the "PDF" or "HTML" hyperlink next to "Trends in Machine-to-Machine Communications") (discussing the growing field of machine-to-machine connected devices including their application in the transportation sector).

[85] *See A Conversation with ITS America President David Hensing*, 11 GLOBAL POSITIONING & NAVIGATION NEWS, no. 11 (May 30, 2001); *ITS America's Fair Information and Privacy Principles*, ITS AM., 1-3, http://www.itsa.org/images/mediacenter/itsaprivacyprinciples.pdf (last visited Oct. 4, 2011); *see also Connected Vehicles – Next Generation ITS*, ITS AM., http://www.itsa.org/forumstaskforcesworkinggroups/connectedvehicle (last updated Aug. 31, 2011).

[86] *See ITS America's Fair Information and Privacy Principles*, ITS AM., 1, http://www.itsa.org/images/ mediacenter/itsaprivacyprinciples.pdf (last visited Oct. 4,

provide an example of how membership organizations across various industries have made an effort to self-regulate on the issue of data security and privacy protection.

III. THE VIRGINIAN LANDSCAPE

[23] While the Virginia Constitution expresses no right of privacy, Article I, Section 10 protects individuals from general warrants for search and seizure.[87] In addition, the courts in Virginia have decided a number of cases that address the issue of the expectation of privacy, including *Atkins v. Commonwealth*, which reiterated the standard for recognizing expectations of privacy.[88] "[T]he test is whether the appellant objectively had a reasonable expectation of privacy at the time and place of the disputed search."[89] A court must "look to the totality of the circumstances" to determine whether an expectation of privacy is objectively reasonable.[90]

2011) ("These principles are advisory, intended to educate and guide transportation professionals . . . .").

[87] VA. CONST. art. 1, § 10 ("That general warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive, and ought not to be granted.").

[88] Atkins v. Commonwealth, 698 S.E.2d 249 (Va. Ct. App. 2010).

[89] *Id.* at 254 (quoting McCoy v. Commonwealth, 343 S.E.2d. 383, 385 (Va. Ct. App. 1986)).

[90] *Id.* These circumstances include:

> whether the defendant has a possessory interest in . . . the place searched, whether he has the right to exclude others from that place, whether he has exhibited a subjective expectation that it would remain free from governmental invasion, whether he took normal precautions to maintain his privacy and whether he was legitimately on the premises.

Id. (quoting *McCoy*, 343 S.E.2d at 385).

[24] A number of cases involving transportation apply this reasonableness standard, most notably as it relates to automobile searches using advanced technology.[91] In the decision announced in *Foltz v. Commonwealth*, the court established that the placement of a Global Position Tracking (GPS) tracking device inside the bumper of the defendant's work van did not constitute a Fourth Amendment "search" or "seizure" and did not violate the defendant's privacy rights.[92] Likewise, the court in *Londono v. Commonwealth* applied the standard in the area of public transportation.[93] Here, the court held that an individual, while traveling on a train "does not enjoy the same expectation of privacy as he would at home."[94] The court went on to explain that, although "occupants of train roomettes may properly expect some degree of privacy," for Fourth Amendment purposes, "it is less than the reasonable expectations that individuals rightfully possess in their homes or their hotel rooms."[95] Also, because "passengers in sleeping cars are repeatedly subject to inquiry and oversight by conductors and other railroad personnel," and "[i]ntrusions such as these necessarily reduce privacy interests," an individual should not expect the same degree of privacy had they decided to stay at home.[96]

[25] The General Assembly of Virginia has enacted several important statutes relating to privacy interests regarding the collection of data by the

[91] *See* United States v. Hernandez, 647 F.3d 216, 219 (5th Cir. 2011); United States v. Cuevas-Perez, 640 F.3d 272, 273 (7th Cir. 2011); United States v. Bailey, 628 F.2d 938, 945 (6th Cir. 1980).

[92] *See* Foltz v. Commonwealth, 698 S.E.2d 281, 287, 289, 290, 292-93 (Va. Ct. App. 2010).

[93] *See* Londono v. Commonwealth, 579 S.E.2d 641 (Va. Ct. App. 2003).

[94] *Id*. at 650 (citing United States v. Whitehead, 849 F.2d 849, 854 (4th Cir. 1988)).

[95] *Id.* (quoting *Whitehead*, 849 F.2d at 853).

[96] *Id.* at 650-51 (quoting *Whitehead*, 849 F.2d at 853).

government.[97] The Government Data Collection and Dissemination Practices Act ("Data Collection Act") recognizes that "an individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information" and acknowledges the vast amount of information now accessible electronically.[98] As such, the Data Collection Act provides a cause of action for using data or acquiring it improperly, as well as allowing for attorneys fees and injunctive relief for individuals adversely impacted per the Act, thus taking steps to ensure the protection of privacy of individuals throughout the Commonwealth.[99] Section 2.2-3800 provides guidelines for recordkeeping agencies of the Commonwealth including: prohibition against secret record keeping systems, prohibition against collection unless there is clear notice stated in advance, and prohibition from collecting personal information except as explicitly or implicitly authorized by law.[100] The Data Collection Act also provides individuals an effective way to correct any collected information about them.[101] In at least one reported case, the legal standard for the government's authority to collect personal data was raised.[102] However, because the Virginia Supreme Court determined the Act did not cover the particular government entity, it was not necessary for the court to reach further into an interpretation of the statute.[103]

---

[97] *See generally* Virginia Freedom of Information Act, VA. CODE ANN. §§ 2.2-3700 to -3714 (2008); Government Data Collection and Dissemination Practices Act, VA. CODE ANN. §§ 2.2-3800 to -3809 (2008); Virginia Computer Crimes Act, VA. CODE ANN. §§ 18.2-152.1 to -152.14 (2009).

[98] VA. CODE ANN. § 2.2-3800.

[99] *See id.* § 2.2-3809.

[100] *Id.* § 2.2-3800(C).

[101] *Id.* § 2.2-3800(C)(7).

[102] *See* Carraway v. Hill, 574 S.E.2d 274, 275 (Va. 2003).

[103] *Id.* at 276-77 (citing Connell v. Kersey, 547 S.E.2d 228, 231-32 (Va. 2001)) (establishing that although the city treasurer provided a newspaper reporter with information from a city treasury employee's employment file, Government Data

[26] In the context of motor vehicles, the 2011 Session of the General Assembly considered and passed S. 946, a bill to augment Section 46.2-844, which allows local school systems to install and operate a video monitoring system on school buses in order to detect drivers who pass a stopped school bus in violation of Section 46.2-859.[104] The statute defines a "video monitoring system" as a system "with one or more camera sensors and computers that produces live digital and recorded video" of motor vehicles which passed school buses as they stop for students.[105] The section also requires the system to record an image of the license plate and the time, date, and location of the vehicle.[106]

[27] The General Assembly, along with those other states who followed California's lead,[107] has enacted legislation regulating event data recorders.[108] In particular, Section 46.2-1088.6 provides that only the owner of the vehicle or one with the consent of the owner's agent or legal representative may access recorded data from a recording device.[109] The statute defines "recording device" as "event data recorders (EDRs), sensing and diagnostic modules (SDMs), electronic control modules

Collection and Dissemination Practices Act did not apply to a treasurer, "a constitutional officer" who "is an independent public official [and] whose authority is derived from the Constitution of Virginia even though the duties of the office may be prescribed by statute").

[104] 2011-838 Va. Adv. Legis. Serv. 1 (LexisNexis) (codified as amended at VA. CODE ANN. § 46.2-844 (Supp. 2011)).

[105] VA. CODE ANN. § 46.2-844(B) (Supp. 2011).

[106] *Id.*

[107] *See generally* ME. REV. STAT. ANN. tit. 29-A, § 1972 (2007); WASH. REV. CODE ANN. § 46.35.030 (West Supp. 2011).

[108] *See generally* VA. CODE ANN. § 46.2-1088.6 (2010).

[109] *Id.* § 46.2-1088.6(B).

(ECMs), automatic crash notification (ACN) systems, geographic information systems (GIS), and any other device that records and preserves data that can be accessed related to that vehicle."[110] Nevertheless, this Section provides exceptions to the general rule requiring consent by the owner or representative.[111] The statute allows for access to recorded data: (1) if the owner or owner's agent has a contract with a third party subscription service that requires access to the device(s); (2) if a licensed new motor vehicle dealer, or mechanic or technician requires access to recorded data to perform ordinary diagnosing, servicing and repair duties; (3) if the recorded data is accessed by an emergency response provider and the data is used to perform emergency response services; (4) if requested by authority of a court of competent jurisdiction; and (5) if the data law enforcement accesses the data in the course of a constitutionally permissible investigation, in accordance with the law regarding searches and seizures.[112] While the statute makes clear the scope of the permissible use of data retrieved from the recorder, there are no civil or criminal liability provisions to protect the owner from unauthorized use by "hacking in" to the data or by law enforcement acting beyond the scope of a Fourth Amendment search or seizure.[113]

[28] In a pair of unpublished companion cases, *Nininger v. Commonwealth*[114] and *Dupree v. Commonwealth*,[115] law enforcement accessed the EDRs from a Hummer H3's and a Chevy Avalanche "using a

[110] *Id.* § 46.2-1088.6(A)(6).

[111] *See id.* § 46.2-1088.6(B)(1)-(5).

[112] *Id.*

[113] *See generally* VA. CODE ANN. § 46.2-1088(B)(1)-(5).

[114] Nininger v. Commonwealth, No. 0450-09-3, 2010 WL 1752572 (Va. Ct. App. May 4, 2010).

[115] Dupree v. Commonwealth, No. 0519-09-3, 2010 WL 1752581 (Va. Ct. App. May 4, 2010).

Crash Data Retrieval System connected to the diagnostic port of the vehicle."[116] The data showed that Nininger was "traveling at 37 mph and never attempted to brake or swerve to avoid the blade of the backhoe"[117] and Dupree "was traveling at 38 mph and he applied his brakes a half-second before he collided with Nininger."[118] Both defendants did not specifically contest the admissibility of the EDR data.[119] These cases suggest that EDR data may be used by law enforcement to search and seize electronic evidence obtained from emerging technology.[120] The court's tacit acceptance of EDR data has created a variety of new legal issues, which in turn requires new legislation to protect the privacy rights of Virginia motor vehicle drivers.[121]

[29] For example, Section 38.2-2212 provides that no insurer shall refuse to renew a motor vehicle insurance policy because of the refusal of an owner of a motor vehicle to provide access to recorded data from a recording device as defined by Section 46.2-1088.6.[122] Section 38.2-2213.1 also provides that when an owner does deny access to recorded data from a recording device, an insurer may not "reduce coverage,

[116] *Dupree*, 2010 WL 1752581, at *3 n.3; *Nininger*, 2010 WL 1752572, at *3 n.3.

[117] *Nininger*, 2010 WL 1752572, at *3.

[118] *Dupree*, 2010 WL 1752581, at *3.

[119] *See Nininger*, 2010 WL 1752572; *Dupree*, 2010 WL 1752581.

[120] *See* Douma & Deckenbach, *supra* note 8, at 314 ("Courts, however, have manifested a willingness to accept data collected by these [EDR] systems in civil cases as long as it complies with the applicable evidentiary standard of 'general acceptance' as a legitimate technology.").

[121] *See, e.g.*, Kevin J. Powers, *David Hasselhoff No Longer Owns the Only Talking Car: Automotive Black Boxes in Criminal Law*, 39 SUFFOLK U. L. REV. 289, 305-08 (2005) (discussing the Fourth and Fifth Amendment concerns implicated regarding the seizure and admissibility of EDR evidence in criminal cases).

[122] VA CODE ANN. § 38.2-2212(C)(1)(s) (2007); VA CODE ANN. § 46.2-1088.6 (2010).

increase the insured's premium, apply a surcharge, refuse to apply a discount . . . place in a less favorable tier" or take other similar negative action solely on the basis of the owner's refusal to allow access to recorded data.[123]

[30] Vehicular tolling facilities have utilized emerging technology to collect vehicular tolls in a faster, more efficient manner.[124] The use of systems such as EZPASS to collect tolls by reading data from the front windshield of the vehicle as it passes through a tolling facility has become increasingly popular in Virginia and across the United States.[125] Not surprisingly, the General Assembly has legislated in this area.[126] Section 46.2-819.1 provides for the installation and use of a photo-monitoring system or an automatic vehicle identification system in certain toll facilities.[127] This section provides that an "operator of any toll facility or the locality within which such toll facility is located may install and operate or cause to be installed and operated a photo-monitoring system or automatic vehicle identification system, or both . . . ."[128] This affords the toll operator the ability to "send an invoice or bill for unpaid tolls to the registered owner of a vehicle as part of an electronic or manual toll collection process . . . ."[129] Section 46.2-819.1 also provides that any data

[123] VA. CODE ANN. § 38.2-2213.1 (2007).

[124] *See* Bob E. Lype, *Employment Law and New Technologies: Emerging Trends Affecting Employers*, 47-MAY TENN. B.J. 20, 24 (2011) ("[T]he 'EZPass' system . . . allows employees to pass toll gates on toll roads without stopping.").

[125] *Cf.* Ian Goldberg, Austin Hill & Adam Shostack, *Trust, Ethics, and Privacy*, 81 B.U. L. REV. 407, 420 (2001) ("The [EZPass] system is coercive in nature, insofar as toll systems become more efficient and failure to participate in the program results in a substantial cost in time.").

[126] *See, e.g.*, VA. CODE ANN. § 46.2-819.1 (2010); VA. CODE ANN. § 46.2-819.5 (2010).

[127] *See* VA. CODE ANN.§ 46.2-819.1(A).

[128] *Id.*

[129] *Id.*

collected by these systems is "limited exclusively to that information that is necessary for the collection of unpaid tolls," and notwithstanding any other provision of law, toll operators may not sell solicit, market for any purpose, or disclose the data to any entity other than for toll collection purposes.[130] Furthermore, it does not permit the data to be introduced as evidence in a court of competent jurisdiction, unless the court action is for determining a violation of Section 46.2-819.1.[131]

[31] Finally, Section 46.2-819.5 provides for the use of photo-monitoring or automatic vehicle identification systems in conjunction with the usage of the Dulles Access Highway to determine violations of a Metropolitan Washington Airports Authority regulation regarding usage of the highway for non-airport purposes.[132] The section has the same requirements and exceptions for the usage of the data collected, including photographs, microphotographs, and electronic images, as does Section 46.2-819.1 explained above.[133] It also requires the purging of data within 30 days after the collection and reconciliation of fees and penalties.[134]

[32] Although Virginia's statutes direct the purging of data collected by these automated systems no later than thirty days after collection and reconciliation of unpaid tolls, as is also the case of data collected by the EDRs,[135] this use of emerging technology for transportation related purposes directly impacts the extent to which an individual can expect to maintain privacy while traveling. There also exists a greater potential for

---

[130] *Id.* § 46.2-819.1(B).

[131] *Id.*

[132] VA. CODE ANN. § 46.2-819.5 (2010).

[133] *Id.* § 46.2-819.5 (B); *see id.* § 46.2-819.1.

[134] *Id.* § 46.2-819.5(B).

[135] *Id.* § 46.2-1088.6(A).

improper use of this data by law enforcement, as compared to traditional or non-technological methods.[136]

IV. CONCLUSION

[33] The rapid advancement of technological innovation in all areas of our society has created new opportunities for resolving the challenges of the 21st century. We have faster and greater access to information in the global village through use of the Internet and its applications. We also have more developed methods for accessing goods and services electronically.[137] In the transportation area, using technology has enabled faster and greater access to services, the ability to transfer more quickly from one mode to another, as well as more choices regarding which mode can be accessed and when.[138]

[34] These positive outcomes from technological innovation, however, have their downsides, including the potential for abuse of the individual's privacy interests.[139] Faster access to transportation has encouraged the electronic collection and maintenance of personal and vehicle data.[140] The

[136] *See generally* Don Oldenburg, *The Snoop in Your Coupe*, WASH. POST, Sept. 9, 2003, at A01 (discussing concerns about use of EDR by law enforcement).

[137] *See, e.g.*, AMAZON.COM, http://www.amazon.com/ (last visited Sept. 2, 2011); ANGIE'S LIST, http://www.angieslist.com/ (last visited Sept. 2, 2011).

[138] *See* Carla Saulter, *Does Better Technology Equal Better Transportation Choices?*, CHOOSE YOUR WAY BELLEVUE BLOG (Mar. 31, 2011, 11:50 AM), http://www.chooseyourwaybellevue.org/blog/2011/03/does-better-technology-equal-better-transportation-choices/.

[139] *See* Patrick R. Mueller, Comment, *Every Time You Brake, Every Turn You Make--I'll Be Watching You: Protecting Driver Privacy in Event Data Recorder Information*, 2006 WIS. L. REV. 135, 166-67 (discussing the high value of EDR to parties involved in Civil and Criminal litigation).

[140] *See* Noam Cohen, *As Data Collecting Grows, Privacy Erodes*, N.Y. TIMES, Feb. 16, 2009, http://www.nytimes.com/2009/02/16/technology/16link.html (discussing services such as Zipcar and go520).

ability to employ symbiotic technological devices has improved the government's ability to enforce the laws and investigate accidents to determine responsibility and/or liability.[141] In the wake of the events of 9/11 and the increase in concern about national security,[142] individual rights have often been violated in protection of the homeland.

[35] This discussion has outlined instances where advancing technology has pushed the limits of personal privacy. The Supreme Court of the United States found in the United States Constitution a "zone of privacy,"[143] but has since created a body of law that sets forth no clear pattern as to the limits of an individual's reasonable expectation to protect their privacy, or the acceptable limits of government action. Congress has enacted legislation, executive branch agencies have promulgated regulations, and industry groups have set standards to guide the access, handling, and disposition of personal information collected through transportation-related technology.[144] Generally, these standards make strong efforts to minimize violations of personal privacy and set forth clear guidelines governing the release and dissemination of personal data.[145] However, these patchwork guidelines often permit the release of personal information, otherwise thought to be private, to achieve public

[141] *See* Oldenburg, *supra* note 136 (providing multiple examples of where EDR was used to convict criminals for driving related offenses).

[142] *See* Bennie G. Thompson, *The National Counterterrorism Center: Foreign and Domestic Intelligence Fusion and the Potential Threat to Privacy*, 6 U. PITT. J. TECH. L. & POL'Y 6, paras. 1, 7, 14 (2006).

[143] *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

[144] *See, e.g.*, Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (2006); 49 C.F.R. §§ 563.1, 563.2 (2010).

[145] *See* 18 U.S.C. §§ 2721-2725.

purposes such as protecting the health and safety of traveling individuals.[146]

[36] The legal landscape in Virginia reflects the federal standards for EDRs,[147] and yet remains distinctive through legislation such as The Government Data Collection and Dissemination Practices Act.[148] In at least two cases, Virginia courts allowed data from EDR equipment admitted into evidence in a criminal proceeding,[149] and held that travelers on public transportation modes have a lesser expectation of privacy than they do in hotel rooms or at home.[150] Virginia permits the use of symbiotic technological applications, photo-monitoring systems, and automatic vehicle identification systems to collect tolls and enforce transportation regulations.[151] However, with the exception of a handful of limited purposes, Virginia permits public disclosure of personal data.[152]

[37] Taken as a whole, the Supreme Court of the United States, Congress and federal agencies, and Virginia's courts and lawmakers have recognized the challenges that emerging technological applications have brought and have permitted this technology to be utilized in a number of ways, including law enforcement, while at the same time attempting to

[146] *See id.* § 2721(b); *ITS America's Fair Information and Privacy Principles*, ITS AM., 2, http://www.itsa.org/images/mediacenter/itsaprivacyprinciples.pdf (last visited Oct. 4, 2011).

[147] *See* VA. CODE ANN. § 46.2-1088.6 (2010).

[148] *See* VA. CODE ANN. § 2.2-3800to -3809 (2008 & Supp. 2010).

[149] *See* Dupree v. Commonwealth, No. 0519-09-3, 2010 WL 1752581, at *3, *3 n.3 (Va. Ct. App. 2010); Nininger v. Commonwealth, No. 0450-09-03, 2010 WL 1752572, at *3, *3 n.3 (Va. Ct. App. 2010).

[150] *See* Londono v. Commonwealth, 579 S.E. 2d 641, 650-51 (Va. Ct. App. 2003).

[151] *See* VA. CODE ANN. §§ 46.2-819.1, -819.5 (2010 & Supp. 2011).

[152] *See id.*

ensure secure data collection.[153] Although methods to protect personal data have been legally prescribed, lawmakers should recognize that the same technological innovations and applications that enabled society to advance may also hinder these protections and violate an individual's legally protected privacy interests.[154]

[38] For example, electronic tolling systems are "rife with privacy risks" and that anyone with a transponder reader can "steal the ID number off transponders . . . through the windshield [of a parked car], put the data on their device[ ] and pass through . . . tolls for free, with the victim paying the bill."[155] Moreover, it is common to "hack" into databases or "phish" into email accounts to steal personal data, including credit card and bank account numbers. As is usually the case, the law lags behind cutting edge innovations that impact individual rights.[156] Emerging technology in transportation proves no exception.[157]

[39] This article supports the conclusion that, in the face of technology advancements, greater efforts by the Congress and the General Assembly of Virginia have protected the personal privacy of the individual by prescribing that collected data must be kept secure and not disseminated

[153] *See, e.g.*, 49 C.F.R. §§ 563.1, 563.2 (2010). *See generally supra* Parts II-III.

[154] *See* Kyllo v. United States, 533 U.S. 27, 33-34 (2001) (imposing limits on the government's power to use thermal imaging technology to "shrink the realm of guaranteed privacy" by conducting a warrantless search of a home).

[155] Elinor Mills, *Hacking Electronic-Toll Systems*, CNET NEWS (Aug. 6, 2008, 4:37 PM), http://news.cnet.com/ 8301-1009_3-10009353-83.html.

[156] *See Kyllo*, 533 U.S. at 33–34 ("It would be foolish to contend that the degree of privacy secured to citizens . . . has been entirely unaffected by the advance of technology.").

[157] *See* People v. Weaver, 12 N.Y.3d 433, 447 (N.Y. 2009) (indicating that advances in GPS monitoring and other technological innovations call for judicial oversight to mitigate the significant risk of abuse).

except for narrow purposes.[158] A second conclusion purports that, as technology is utilized to enforce speed limits and red light violations, collect tolls and enforce roadway restrictions, the public will challenge those intrusions. As our system requires, the outcomes to these challenges is still unfolding in the courts.[159] One thing is clear however, enforcement of the law through more sophisticated technological methods causes the individuals affected to bristle at the government's broader reach.[160] As one motorist, who received a ticket in the mail from Ridgeland, South Carolina—a town that employs speed cameras to enforce the speed limit on I-95 said: "I just don't think it's right. If you get a ticket you should be stopped by an officer, know you have been stopped and have an opportunity to state your case."[161]

[40] While traveling in the "circulatory system"[162] of the United States, is the right of privacy sacrificed for the health and convenience of the transportation system? Has transportation technology struck the final nail into the coffin of personal privacy? This article has shown that our legal institutions, which at times seem poised to summon the hearse, must continually respond to a public that heralds individual liberties and demands that privacy rights remain recognized, placed on life support, and protected.

---

[158] *See, e.g.*, 49 C.F.R. §§ 563.1, 563.3 (2010); VA. CODE ANN. § 46.2-819.1(B)(i)-(iv) (2010 & Supp. 2011).

[159] *See* City of Davenport v. Seymour, 755 N.W.2d 533, 536 (Iowa 2008) (noting variations in the acceptance of automated traffic enforcement systems among state legislatures).

[160] *See* Bruce Smith, *I-95 Cameras Snap Speeders, Spark Controversy*, MSNBC.COM (Mar. 27, 2011, 12:28 PM), http://www.msnbc.com/id/42294692/ns/us_news-crime_and_courts/.

[161] *Id.*

[162] IBM, SMARTER TRANSPORTATION, *supra* note 1, at 2.