

# Santa Clara High Technology Law Journal

Volume 11 | Issue 1 Article 6

January 1995

# The Traffic in Souls: Privacy Interests and the Intelligent Vehicle-Highway Systems

Sheldon W. Halpern

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj



Part of the Law Commons

# Recommended Citation

Sheldon W. Halpern, The Traffic in Souls: Privacy Interests and the Intelligent Vehicle-Highway Systems, 11 Santa Clara High Tech. L.J. 45 (1995).

Available at: http://digitalcommons.law.scu.edu/chtlj/vol11/iss1/6

This Symposium is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.

# THE TRAFFIC IN SOULS: PRIVACY INTERESTS AND THE INTELLIGENT VEHICLE-HIGHWAY SYSTEMS

## Sheldon W. Halpern†

IVHS can improve safety, reduce congestion, enhance mobility, minimize environmental impact, save energy, and promote economic productivity in our transportation system. It will multiply the effectiveness of future spending on highway construction and maintenance and will increase the attractiveness of public transportation. IVHS will be as basic a transportation raw material as concrete, asphalt, or steel rail.<sup>1</sup>

\* \* \*

[S]cientific and technological advances have raised the spectre of new and frightening invasions of privacy. Our capacity as a society to deal with the impact of this new technology depends, in part, on the degree to which we can assimilate the threat it poses to the settled ways our legal institutions have developed for dealing with similar threats in the past.<sup>2</sup>

#### I. Introduction

The development of The Intelligent Vehicle-Highway System (IVHS) is serious business. Notwithstanding visions of high-tech circuitry producing a low comedy circus, there is a real and expensive long-term commitment to the refinement and implementation of IVHS. "Over the next 20 years, a national IVHS program could have a greater societal impact than even the Interstate Highway System."

Copyright © 1994 by Sheldon W. Halpern

<sup>†</sup> Professor of Law, The Ohio State University College of Law. B.A., 1957 Cornell University; L.L.B., 1959 Cornell University. For her analysis, questioning, advice, and support I wish to thank Dr. Dorit Samuel.

<sup>1.</sup> IVHS Architecture Dev. Program, Interim Status Report 2 (April, 1994) [here-inafter IVHS Architecture].

Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L. Rev. 962, 963 (1964) (footnote omitted).

<sup>3.</sup> IVHS ARCHITECTURE, supra note 1, at 2.

From significant federal funding<sup>4</sup> to the creation of a voluminous *Strategic Plan* by IVHS America, a consortium of private industry, academia and other institutions seeking to define and, by so doing structure and direct, the nature and content of IVHS,<sup>5</sup> one can see that the stakes are high and the players powerful. In short, there is much more than smoke, mirrors and a cosmetic political attempt to capitalize on an infatuation with technology.<sup>6</sup>

Conceptually, IVHS has significant potential, even if so far the laboring financial oar has been borne by the government; private sector hard commitment remains elusive and well short of what had been contemplated.<sup>7</sup> The technology contemplates a structure in which "roadways, vehicles, and travelers are integrated into a single in-

4. See Joseph Sussman and Hans Klein, What the IVHS Strategic Planning Process Taught the Planners, IVHS Rev. 9, 19 (1993). "In 1991 Congress authorized \$660 million of federal funds for IVHS activities over the following six years. A second piece of legislation authorized an additional \$170 million for 1992 and 1993." By 1993 President Clinton proposed increasing this authorization to \$925 million from fiscal year 1994 through 1997. Kristine M. Williams, IVHS: Smart Cars, Smart Highways, ALI-ABA COURSE OF STUDY, LAND USE INSTITUTE: PLANNING, REGULATION, LITIGATION, EMINENT DOMAIN, AND COMPENSATION, C851 ALI-ABA 627, 683 (1993). Ms. Williams suggests that

Federal support for IVHS appears to have evolved in part from the desire to redirect defense industries in the post-military industrial complex toward domestic projects. IVHS spending aims to focus high tech innovations on improving the efficiency and safety of the surface transportation system. By providing the opportunity for new contracts to corporations previously receiving defense dollars, IVHS also promises to preserve jobs and help rebuild the nation's sagging economy.

Id.

5. IVHS AMERICA, STRATEGIC PLAN FOR INTELLIGENT VEHICLE-HIGHWAY SYSTEMS IN THE UNITED STATES, Report No. IVHS-America-92-3 (1992) [hereinafter Strategic Plan]. See also IVHS Architecture, supra note 1.

IVHS AMERICA is a public/private partnership encompassing all levels of government, the private sector, professional associations, and the universities, in a joint effort to define and advance a national IVHS program for more efficient, safer, and environmentally sound road transport through research, development, testing, and implementation of advanced technology. IVHS AMERICA's role is to define IVHS goals for North America, facilitate IVHS coordination across jurisdictional and sector boundaries, identify and oversee the development of relevant standards, and provide reliable information on IVHS to the general public.

Primer on Intelligent Vehicle Highway Systems, Transportation Research Circular 8 (Aug., 1993) (hereinafter Primer).

- 6. See, e.g., IVHS Architecture, supra note 1, at 2:
- IVHS is not a distant vision. Already, real systems, products, and services are being tested throughout the U.S. Some first-generation systems are on the market or in the final stages of development. More than 20 real-world operational tests are now under way or are planned as federal/state/private ventures to evaluate more advanced IVHS concepts and components.
- 7. "The national program seems to be unfolding as a public sector development program .... Evidence for fulfillment of the prediction of overwhelming private sector investment in IVHS (80 percent of the total) is not yet apparent." Sussman and Klein, supra note 4.

termodal system." The presently contemplated modules to be integrated include Advanced Traffic Management Systems, Advanced Traveler Information Systems, Advanced Vehicle Control Systems, Commercial Vehicle Operations, Advanced Public Transportation Systems and Advanced Rural Transportation Systems. Field testing of components of the system is well underway. When and if the parts become fully integrated and operational, there will be in place, on the one hand, an integrated highway directional, safety and control system and, on the other, a technology by which vehicles—presumably with occupants—may be tagged and tracked and the information generated by that tracking stored, manipulated, and used. Hence the concern over privacy, a concern with significant political and financial implications for the entire project.

In its Strategic Plan, IVHS AMERICA acknowledges that privacy protection must be considered "to assure program integrity and credibility and to secure public acceptance and support." At the same time, the Plan cautions that privacy "[l]imitations and protections on the use of data collected in IVHS that might help in the finance of programs could . . . limit opportunities for its beneficial use, both for public sector planning and for commercialization." <sup>13</sup>

Appropriate safeguards and guidelines on the control and use of IVHS information must... be built into the process in order to alleviate concerns over the inappropriate use of the data and in order to protect the privacy of individual vehicle users.

As Miller observed more than twenty years ago:

Close scrutiny and evaluation of the implications of information technology on individual privacy are especially appropriate... because of the rising interest in many quarters for the establishment of governmental and private data centers. The extent to which federal agencies and private companies are using computers... to collect, store, and exchange information about the activities of private citizens is rapidly increasing.

Arthur B. Miller, Computers, Data Banks and Individual Privacy: An Overview, 4 Colum. Human Rights L. Rev. 1, 3 (1972). See George B. Trubow, Protecting Informational Privacy in the Information Society, 10 N. Ill. U.L. Rev. 521, 527(1990) ("It is clear that new information and communication technologies pose serious threats to informational privacy in both the public and private sectors").

<sup>8.</sup> Id. at 17.

<sup>9.</sup> Id. at 11.

<sup>10.</sup> See Primer, supra note 5 at 13-16; see also IVHS ARCHITECTURE, supra note 1, at 3.

<sup>11.</sup> See, e.g., the Strategic Plan, supra note 5, at III-128:

<sup>12.</sup> Strategic Plan, supra note 5, at III-128. See also IVHS Architecture, supra note 1, at 22.

<sup>13.</sup> STRATEGIC PLAN, supra note 5, at III-129.

#### II. THE PRIVACY PROBLEM

The very phrase "Intelligent Vehicle-Highway Systems" polarizes. As an immediate example of computer controlled observation, data collection and activity direction, it evokes the duality that seems to attend the interface between high technology and human activity.<sup>14</sup> One is instinctively drawn either to utter a reverential paean to the gods of technology who will make our automobile-driven lives richer. safer and more accurate, if not more scenic, or to mutter luddite imprecations spiced salaciously with reference to a not-so-benign "big brother". Here we are presented with the prospect of a vast (read pervasive and intrusive) network (read spider web) of nurture and guidance (suspicion and surveillance) that will ensure our safety and security (subservience and conformity) by means of unobtrusive (secret) technological systems. One anticipates the millennium with either wonder and awe or dread and foreboding—we eagerly await or we view with alarm. Discussion and the formulation of policy will all too often be predicated on one or the other of these underlying mindsets.

When considering the privacy implications of technological change we tend to focus on the dramatic. The celebrity-hero pursued by the police tracked through triangulation of cellular telephone signals originating from the car in which he is a passenger<sup>15</sup> captures a huge television audience that watches the balletic pursuit from the vantage point of a hovering helicopter. The immediacy and intimacy are inescapable as is the sense of dislocation of reality. The fascination with watching—witnessing the private—ranges, of course, from the mundane act of secretly investigating the contents of a friend's bathroom medicine cabinet to the much less benign act of stalking.

<sup>14.</sup> See Philip E. Agre, Surveillance and Capture: Two Models of Privacy, 10 The Information Society 101 (1994):

As Kling and Dunlop (1993) have pointed out, analysis of the place of computer technology in society has often been impoverished through a bifurcation into two structurally opposed genres, which they call utopian and anti-utopian. The utopian genre, as its name suggests, emphasizes good things: efficiency, the amplification of various professions' powers, and other beneficial consequences of computing. The anti-utopian genre, for its part, draws on a stock of cultural images of class conflict and totalitarian domination. Both genres are prevalent in journalistic and academic writing alike.

Id. at 115.

<sup>15.</sup> Simpson, Under Suicide Watch, is Jailed After a Bizarre Chase, N.Y. TIMES, June 19, 1994, at 1, col. 2 (Nat'l Ed.).

<sup>16.</sup> Because we are watching we become part of the scene, an audience that increasingly may be unable to distinguish reality from "entertainment." The act of watching, of making the private act a public one may itself transform both the watchers and the watched.

Thus, it is not at all surprising that the association that springs from the idea of a system that facilitates the identification, locating and tracking of a passenger vehicle, is that of watching. In short, as noted by Philip Agre, <sup>17</sup> the model of privacy that first suggests itself in this context is that of surveillance—the flying goose has been tagged and can no longer hide or freely fly.

To be sure, the matter of surveillance should not be trivialized.<sup>19</sup> There is reason to be concerned about systems that could facilitate state control by means of tagging devices that locate and track individuals. The fact that a vehicle, rather than its occupant, is the tagged and tracked object is, as a matter of reality, irrelevant. For most purposes,

- 17. Agre, supra note 14.
- 18. Id. at 101, 107. Agre defines the model further:

The surveillance model has five components:

- (1) visual metaphors, as in Orwell's "Big Brother is watching you" or Bentham's Panopticon;
- (2) the assumption that this "watching" is nondisruptive and surreptitious (except perhaps when going astray or issuing a threat);
- (3) territorial metaphors, as in the "invasion" of a "private" personal space, prototypically the family home, marked out by "rights" and the opposition between "coercion" and "consent";
- (4) centralized orchestration by means of a bureaucracy with a unified set of "files"; and
- (5) identification with the state, and in particular with consciously planned-out malevolent aims of a specifically political nature.

When stated in this way, it becomes evident that the surveillance model is a cultural phenomenon. Although its earliest genealogy deserves further research, its modern history is clearly rooted in the historical experience of secret police organizations and their networks of listening devices and informers, most prominently in the totalitarian states of Nazi Germany and the Soviet Union, and to a lesser but still significant extent in the United States. George Orwell's 1984 gave these symbols their most vivid literary form, but the cultural legacy of this history is also evident in, for example, the unpleasant connotations associated with certain uses of a word like "files".

#### Id. at 105-106.

19. Spiros Simitis, Reviewing Privacy in an Information Society, 135 U. Pa. L. Rev. 707, 726-29 (1987). "[B]ecause of both the broad availability of personal data and the elaborate matching procedures, individual activities can be accurately reconstructed through automated processing. Surveillance becomes the order of the day." Id. at 726.

tracking my car is tracking me.<sup>20</sup> So too, the law has recognized the actionability of certain kinds of "overzealous" surveillance.<sup>21</sup>

Concomitant with tracking is compilation of personal information. With surveillance comes the "dossier". The modern dossier, the product of sophisticated computer compilation and manipulation of data cannot escape its sinister connotations and images of an omnipresent and information-stuffed controlling presence.<sup>22</sup> Finally, the existence of the watchers and the dossier combine to alter individual behavior to accommodate and conform to the system.<sup>23</sup> The frightening 1984 scenario, again, should not simply be dismissed as a form of anti-technology paranoia. Society must be alert to the threat of centralized accumulated governmental power which may be directed at designated individuals.<sup>24</sup> However, while the twentieth century has

#### 20. See Agre, supra note 14 at 104:

One might further distinguish between systems that track human beings and systems that track physical objects. Such a distinction would be misleading, though. Systems are indeed found at each extreme—for example radio transmitters attached to shipping crates or fastened to prisoners' limbs. But many of the systems track both people and objects, and others track objects as stand-ins for people.

- 21. See Nader v. General Motors Corp., 255 N.E.2d 765, 771 (1970).
- 22. See, e.g., Note, Privacy, Computers, and the Commercial Dissemination of Personal Information, 65 Tex. L. Rev. 1395-96 (1987):

Large databases, when combined with sophisticated programming techniques, enable companies to discover an individual's attitudes, values, interests, and opinions. The same technology that fills mailboxes with advertisements for countless products can facilitate the creation of thorough dossiers documenting a person's private activities.

Because computer technology so dramatically facilitates collecting, storing, processing, and disseminating information, it poses a number of new threats to individual privacy.

#### 23. Id. at 1396:

Knowing that every transaction is forever stored in an electronic database can change an individual's perception of herself and her relationship to society. She knows she can never discard her past, that others will judge her on a computer record. Thus she is apt to assume conformist behavior to maintain a "good" record, avoid "deviant" or controversial activity regardless of her true beliefs and feelings, and reduce her independent action and thought. The concomitant loss of individual diversity saps social vitality. The changes wrought by the use of computers also may have large-scale effects. Power may shift to large bureaucratic institutions with the resources to make full use of the new technology, denying individuals the opportunity to participate in society's most basic transactions. (footnote omitted)

See Simitis, supra note 19, at 710 ("personal information is increasingly used to enforce standards of behavior. Information processing is developing, therefore, into an essential element of long-term strategies of manipulation intended to mold and adjust individual conduct").

- 24. Cf. Privacy Protection Study Commission, Personal Privacy in an Information Society (1977):
  - ... Americans must... be concerned about the long term effect recordkeeping practices can have not only on relationships between individuals and organizations, but also on the balance of power between government and the rest of

witnessed such centralized and totalitarian state activity, the complexity of American society indicates that this response to technology is at once overly dramatic in its focus on malicious state action<sup>25</sup> and simplistic in ignoring the more banal but insidious impact that tracking technology may have on the individual. The IVHS complex, along with cognate systems, implicates a more sophisticated and multivariate set of privacy concerns. With its assumption of significant, if not dominant private industry participation and control, IVHS is not the state centered leviathan spawning a single and sinister "Big Brother". Concomitantly, the lack of a single federal "villain" precludes a single, federal legislative solution.<sup>26</sup>

IVHS contemplates a comprehensive tracking and information compilation system that inevitably raises concerns for the individual "tracked".<sup>27</sup> The various modules of the systems involve or would fa-

the society. Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly. Thus, growth in society's record-keeping capability poses the risk that existing poser balances will be upset.

#### Id. at 6.

#### 25. See Agre, supra note 14, at 116:

When applied as the sole framework of computing and privacy, the surveillance model contributes to the near-inevitability of oversimplified analysis.... Unfortunately, all the surveillance model offers is a metaphor of bureaucratically organized state terror that often seems disproportionate to the actual experience of corporate life. The rhetoric of "Big Brother technologies" is easily—and frequently—ridiculed through paraphrase in terms of "sinister conspiracies" and the like. The paradoxical result is that genuinely worrisome developments can seem "not so bad" simply for lacking the overt horrors of Orwell's dystopia.

#### 26. See Simitis, supra note 19, at 726:

[T]he aim of controlling and adjusting individual behavior is by no means an exclusive attribute of processing activities initiated by the state. [P]rivate enterprises and state agencies resort to automated processing for quite similar purposes.... The boundaries between the public and private sectors are thus blurred. Personal data, once stored, tend to become a flexible, common base of information.

#### 27. Agre describes tracking systems:

In each case, some entity changes state, a computer internally represents those states, and certain technical and social means are provided for (intendedly at least) maintaining the correspondence between the representation and the reality. The computer may maintain a centralized database (this is the usual case) or it may be more widely distributed. Each entity has a definite identity that remains stable over time, and if several entities are being tracked then the tracking system has some means of consistently "attaching" a given entity to its corresponding representation. This representation will be expressed within some mathematically definable representation scheme, which is capable of expressing a certain formal space of states of affairs. The computer maintains a representation only of certain aspects of the entity. In particular, the representation scheme recognizes certain specific kinds of changes-of-state, namely those which correspond to changes in the stored representation. . . . As the entity's corresponding representation

cilitate tracking and the accumulation of information. Advanced Traveler Information Systems, in providing on-board display, guidance, and warning systems provides the basis for individual automobile tracking. Advanced Vehicle Control Systems directly intrudes into the driver's control over the vehicle. Commercial Vehicle Operations, while targeted to commercial vehicles nevertheless put in place direct tagging and monitoring technology through the Automatic Vehicle Identification, Automatic Vehicle Classification, Automatic Vehicle Location, and other sub-systems. Advanced Rural Transportation Systems similarly include Automatic Vehicle Location and route guidance components. Advanced Traffic Management and Advanced Public Transportation Systems, although not keyed to individuals, call for the development of easily expandable control and tracking systems.<sup>28</sup>

Rather than individual surveillance, the tracking technology here is designed to provide behavioral information that in its origin is indifferent to the individual to whom the information relates. In so doing, however, detailed information about the individual activity is captured and stored, in a process that necessarily impacts upon the individual.<sup>29</sup> As the United States Supreme Court has observed, "the power of compilations to affect personal privacy . . . outstrips the combined power of the bits of information contained within."<sup>30</sup> IVHS ultimately involves a system of electronic "watchers" observing and recording individual-specific information which may then be used for a variety of purposes; purposes which, however benign in intent, arise out of individual exposure to the system, in a process that offers an opportunity for exploitation and abuse.

changes, records may well be kept of its state transitions, yielding a "history" of its trajectory through time. And this trajectory, of course, can be either literal or metaphorical, depending on what aspects of the entity are represented.

Tracking systems like these can obviously be used for good or ill. Agre, *supra* note 14 at 104-105.

- 28. Primer, supra note 5, at 5-7.
- 29. See Agre, supra note 14 at 105:

[T]racking schemes have another side: the practical arrangements through which the data is collected in the first place, including the arrangements that make human activities and physical processes trackable. As human activities become intertwined with the mechanisms of computerized tracking, the notion of human interactions with a "computer"— understood as a discrete, physically localized entity—begins to lose its force; in its place we encounter activity-systems that are thoroughly integrated with distributed computational processes,

<sup>30.</sup> United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 765 (1989).

53

Abuse, in its most sinister form—state surveillance and control—is the most glaring, if not the most likely horror scenario. The exploitative, commercial use of individual data for purposes unrelated to the rationale of IVHS is a more insidious and more likely concomitant of the tracking/collection process.31 Beyond these blatant privacy concerns we must consider the impact of the very existence of a highly integrated watching system devoted to what has become for many a core factor in daily living—automobile travel. With or without the possibility of the creation of individually referable data bases, in a variant of the Heisenberg Principle, the fact alone of being observed may modify and control the behavior of the subject of the observation. So too, there is discomfort with a series of interlocked systems capable of accumulating and coordinating data arising from individual tracking. Ultimately, concern exists over the use of retained data, whether by creating product oriented mailing lists targeted to specific driver "profiles" or more personal uses of the detailed behavioral information. On a more general level, "[f]or a democratic society . . . the risks are high: labeling of individuals, manipulative tendencies, magnification of errors, and strengthening of social control threaten the very fabric of democracy."32

In any case, it is the consequence of continuing mass capture<sup>33</sup> and storage of data in the IVHS that drives the privacy inquiry. That

Data-gathering and dossier-building are as prevalent in private industry as in government. Personal information can be used for commercial purposes, such as generating a list of prospective consumers. . . .

The commercial use of cybernetics may go beyond this relatively benign method of soliciting business. The line between using the technology to communicate with a customer and employing it to manipulate his attitudes is nebulous and is likely to be transgressed frequently.

Miller, supra note 11, at 6-7.

32. Simitis, supra note 19, at 746.

33. Thus Agre postulates the "capture model" of privacy:

The term has two uses. The first and most frequent refers to a computer system's (figurative) act of acquiring certain data as input, whether from a human operator or from an electronic or electromechanical device. . . . The second use of "capture", which is more common in artificial intelligence research, refers to a representation scheme's ability to fully, accurately, or "cleanly" express particular semantic notions or distinctions, without reference to the actual taking-in of

The capture model can be contrasted point-by-point with the surveillance model.

<sup>31.</sup> Cf. Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights? 44 FED. COMM. L.J. 195, 207 (1992) ("In fact, Americans today are more distrustful of industry than government with respect to the collection and use of personal information") (footnote omitted).

<sup>(1)</sup> linguistic metaphors for human activities, assimilating them to the constructs of a computer system's representation languages;

inquiry must consider whether the individual about whom data is captured has or should have any rights with respect to (a) the capture process itself—whether, when and how the capture is to occur; (b) the storage process—how, where, and for how long should such data be kept and who is to have access to it; and (c) the dissemination process—for what purposes and how is the data to be used.<sup>34</sup> The issue of use is perhaps the most troubling,35 although each aspect of the tracking/capture complex has implications for individual behavior and rights. Indeed, control over or limitations upon the storage process may well obviate the problems of use.<sup>36</sup> Overall is the question of whether and to what extent an individual has a proprietary interest in personal data. Who, if anyone, "owns" me or, if not me, detailed data about me? The task of the legal system is to find or create appropriate models—privacy or property paradigms—to define individual rights and technological limitations in order both to derive the benefits of the technology and to preserve the societal values that underlie the right of privacy.

It is suggested here that the privacy and property legal complex, as it presently exists, cannot adequately provide the necessary model with universal application and that reconciliation of IVHS and privacy interests can be achieved primarily through ad hoc adjustment in the system itself. The very technology that gives rise to the problem can be the means for limiting, if not obviating the possibility of privacy abuses arising out of that technology.

Agre, supra note 14, at 106-107.

A 1990 poll taken in the United States by Equifax, one of the major national credit reporting agencies, found that seventy-nine percent of Americans are concerned about privacy and the use of personal information [and] seventy-one percent of Americans believe they have lost control over the use and dissemination of personal information.

<sup>(2)</sup> the assumption that the linguistic "parsing" of human activities involves active intervention in and reorganization of those activities:

<sup>(3)</sup> structural metaphors; the captured activity is figuratively assembled from a "catalog" of parts provided as part of its institutional setting;

<sup>(4)</sup> decentralized and heterogeneous organization; the process is normally conducted within particular, local practices which involve people in the workings of larger social formations; and

<sup>(5)</sup> the driving aims are not political but philosophical, as activity is reconstructed through assimilation to a transcendent ("virtual") order of mathematical formalism.

<sup>34.</sup> See Reidenberg, supra note 31.

<sup>35.</sup> As Reidenberg notes:

Id. at 198 (citing Louis Harris Assocs. & Alan F. Westin, Equifax, Inc., the Equifax Report on Consumers in the Information Age, at V (1990) (footnotes omitted).

<sup>36.</sup> See infra notes 117-126 and accompanying text.

# III. PARADIGM LOST: THE RIGHT OF PRIVACY AND COLLECTION AND DISSEMINATION OF INFORMATION

The American legal system does not contain a comprehensive set of privacy rights or principles that collectively address the acquisition, storage, transmission, use and disclosure of personal information within the business community. . . . Instead, legal protection is accorded exclusively through privacy rights created on an ad hoc basis by federal or state legislation or state common law rules.<sup>37</sup>

### A. The Nature of the "Classic" Privacy Tort

"Privacy" is an elusive concept, connoting an array of values, thoughts, aspirations, and fears defying objective unification:

The word "privacy" has taken on so many different meanings and connotations in so many different legal and social contexts that it has largely ceased to convey any single coherent concept. . . . Most people will readily agree that they should have a "right of privacy." But when pressed for a definition, they will give widely varying responses. . . .

It is apparent that the word "privacy" has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts. . . . Like the emotive word "freedom", "privacy" means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.<sup>38</sup>

This paper is concerned with the "privacy" tort, embracing an individual's claim against another who, in exercising an otherwise lawful right, impinges upon that individual's interest in anonymity. As such, the tort must be distinguished from a purported constitutional "right of privacy," which refers to an individual's rights against intrusive governmental action, "the claim that each citizen has a right of autonomy—a right to decide how to live and to associate with others, free from all but the most carefully limited impingements by governmental authority."

<sup>37.</sup> Reidenberg, supra note 31, at 208 (footnotes omitted).

<sup>38.</sup> J.Thomas McCarthy, The Rights of Publicity and Privacy § 1.1[B][1], at 1-3; § 5.7[D], at 5-65 (1992). "The phrase 'a right of privacy' as used in law has almost as many meanings as Hydra had heads." Diane L. Zimmerman, False Light Invasion of Privacy: The Light That Failed, 64 N.Y.U. L. Rev. 364 (1989).

<sup>39.</sup> Zimmerman, supra note 38, at 364. Professor McCarthy suggests that "the only significant thing that the Constitutional right of privacy and the common law right of privacy share is the label." McCarthy, supra note 38, at 5-60-61; but cf. Richard C. Turkington, The Emerging Unencumbered Constitutional Right to Informational Privacy, 10 N. Ill. U.L. Rev. 479 (1990), which elaborates upon a linkage between the tort and constitutional privacy rights.

It has become axiomatic to note that the modern privacy tort began when Samuel Warren and Louis D. Brandeis postulated a common law "right to privacy." As I have suggested elsewhere, the whether such a common-law right, with a concomitant tort remedy, actually existed or was created by the authors, is now more of historical than practical interest, as virtually all jurisdictions now recognize, either by common law or statute, some form of the individual's right to exercise some degree of control over the public use of his or her persona.

The development of the tort has been marked by confusion and controversy over the nature of the right, exemplified by the diverse analytic models of Dean William Prosser and Dr. Edward Bloustein. Dean Prosser postulated a right of privacy embracing "not one tort, but a complex of four different interests." Bloustein argued that Prosser had both misstated and diminished the right of privacy, 47 and sought to bring Prosser's divergent, separate "torts" within a unifying conceptual umbrella, shielding a single interest, "the interest in preserving individual dignity."

<sup>40.</sup> Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. Rev. 193 (1890).

<sup>41.</sup> Sheldon W. Halpern, Rethinking the Right of Privacy: Dignity, Decency, and the Law's Limitations, 43 Rutgers L. Rev. 539 (1991).

<sup>42.</sup> Compare Roberson v. Rochester Folding Box Co., 64 N.E. 442, 447 (N.Y. 1902) with Pavesich v. New England Life Ins. Co., 50 S.E. 68, 80-81 (Ga. 1905).

<sup>43.</sup> See Peter Felcher & Edward Rubin, Privacy, Publicity, and the Portrayal of Real People by the Media, 88 YALE L.J. 1577, 1581 (1979) (suggesting that Warren and Brandeis, "in the process of searching for [a common law right of privacy] succeeded in inventing it"); Zimmerman, supra, note 38, at 364-65 (1989) ("The common law right of privacy was conceived in the late nineteenth century by the fertile intellects of Samuel Warren and Louis Brandeis, and was born on the pages of the Harvard Law Review.")

<sup>44.</sup> See McCarthy, supra note 38, at § 1.3; Jerome A. Barron, Warren & Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation, 13 Suffolk U.L. Rev. 875 (1979); Dorothy Glancy, The Invention of the Right to Privacy, 21 Ariz. L. Rev. 1 (1979).

<sup>45.</sup> See Crump v. Beckley Newspapers, Inc., 320 S.E.2d 70, 82 (W. Va. 1984). See also McCarthy, supra note 38, ch. 6.

<sup>46.</sup> William Prosser, *Privacy*, 48 Calif. L. Rev. 383, 389 (1960). Dean Prosser defined these separate torts as "(1) Intrusion upon the plaintiff's seclusion or solitude . . . . (2) Public disclosure of embarrassing private facts . . . . (3) Publicity which places the plaintiff in a false light . . . . (4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness." *Id.* This theory of distinctive branches off a common privacy root was codified in the RESTATEMENT (SECOND) OF TORTS § 652A (1976) (a section for which Dean Prosser had been the Reporter).

<sup>47.</sup> Bloustein, supra note 2, at 965-66, 970.

<sup>48.</sup> Id. at 986. Bloustein concluded that "the interest protected in each [of Prosser's distinct 'torts'] is the same, it is human dignity and individuality or, in Warren and Brandeis' words, 'inviolate personality.' "Id. at 991. See also Sheldon W. Halpern, the Law of Defamation, Privacy, Publicity and Moral Right 376 (2d ed. 1993) ("Notwithstanding its appearance in opinions, almost as an obligatory prelude to discussion of 'privacy,' there is serious doubt as to

57

[T]he interest served in the privacy cases is in some sense a spiritual interest rather than an interest in property or reputation . . . . [T]he spiritual characteristic which is at issue is not a form of trauma, mental illness or distress, but rather individuality or freedom.

An intrusion on our privacy threatens our liberty as individuals to do as we will, just as an assault, a battery or imprisonment of our person does. . . . [We should] regard privacy as a dignitary tort. . . . The injury is to our individuality, to our dignity as individuals, and the legal remedy represents a social vindication of the human spirit thus threatened rather than a recompense for the loss suffered.<sup>49</sup>

More recently, Professor Robert Post has suggested that the strong moral basis for a right of privacy inheres in our system of community and the respect accorded the individual by the community.<sup>50</sup> To Professor Post, "the common law tort of invasion of privacy offers a rich and complex apprehension of the texture of social life in America."51 His formulation in terms of rules of "civility" extrapolates individual dignity into a complex community norm.<sup>52</sup> It implicates the very fabric of a civilized society:

[T]he plain fact [is] that privacy is for us a living reality only because we enjoy a certain kind of communal existence. Our very "dignity" inheres in that existence, which, if it is not acknowledged and preserved, will vanish, as will the privacy we cherish.<sup>53</sup>

Both Post and Bloustein sought to give legal structure to what they saw as a deeply moral construct. A violation of privacy is a violation of the self, when, as Bloustein compassionately recognized, "[t]he innermost region of being—the soul, if you will—has been bruised by exposure to the world."54

The privacy right underlying the tort has been understood to relate to the bruises to the soul that follow from unwanted public exposure. Classically, it has concerned the unconsented to public use of

the utility and validity of the Prosser quadrupedal analysis, particularly when one considers the interests underlying the different causes of action").

<sup>49.</sup> Bloustein, supra note 2, at 1002-03 (footnote omitted).

<sup>50.</sup> Robert Post, The Social Foundations of Privacy: Community and Self in the Common Law Tort, 77 CALIF. L. REV. 957 (1989). Professor Post builds on the work of Erving Goffman. Erving Goffman, The Nature of Deference and Demeanor, in Interaction Ritual: Essays on FACE-TO-FACE BEHAVIOR 47 (1967).

<sup>51.</sup> Post, supra note 50, at 959.

<sup>52.</sup> Id. at 968.

<sup>53.</sup> Id. at 1010; see also Turkington, supra note 39, at 485-87.

<sup>54.</sup> Edward J. Bloustein, The First Amendment and Privacy: The Supreme Court Justice and the Philosopher, 28 RUTGERS L. Rev. 41, 54 (1974).

another's "name or likeness."<sup>55</sup> The tort is, in essence, a mass communication tort and the interest it protects is the interest in anonymity in terms of public exposure.<sup>56</sup> The personal, emotional, subjective nature of the privacy interest—its relation to the injury to feelings from violated anonymity—has been regularly reaffirmed.<sup>57</sup> The significant difficulty in building an appropriate legal construct to protect this subjective interest has centered around the fact that the harmful public exposure is usually the product of public truthful speech—in short, a conflict between two values, both conflicting and necessary to a free society.<sup>58</sup>

The tension between the competing values has frequently been framed in constitutional terms: how does one regulate or limit truthful speech consistently with First Amendment protection of speech and press. In the context of violation of privacy as a media tort, reconciliation, such as it is, of the conflict has revolved around the elusive concept of "newsworthiness" in connection with mass publication of an individual's name or likeness, either as such or as part of the publication of factual, albeit offensive or embarrassing information about the individual named or depicted.<sup>59</sup> From its inception, the right of pri-

Because the existence of a democratic society depends essentially on an uninhibited proliferation of information, privacy very quickly became one of the main objects of debate. In fact, free speech has been seen, to a substantial extent, as a product of the constant adjustment of the boundary between the individual's right to be let alone and the public's need to be informed. The standard remarks on the relative nature of privacy or on the necessity of a careful balancing of interests are more than significant. Far from being considered a constitutive element of a democratic society, privacy appears as a tolerated contradiction, the implications of which must be continuously reconsidered.

<sup>55.</sup> See HALPERN, supra note 48, at 392. The statutory formula in New York, and several other states, "name, portrait, or picture" (N.Y. Crv. Rights Law § 50 (McKinney 1992)), is not essentially different from the common-law "name or likeness" requirement; see also CAL.Crv.Code § 2233(a) (Deering Supp. 1993) (making actionable the use of someone's voice or signature, as well as name or likeness).

<sup>56.</sup> See generally, McCarthy, supra note 38; Halpern, supra note 48, Part Two—Privacy; Trubow, supra note 11 at 534 ("the tort focuses on publication").

<sup>57.</sup> See, e.g., Fairfield v. American Photocopy Equipment Co., 291 P.2d 194, 197 (Ca. 1955) ("The gist of the cause of action in a privacy case is . . . a direct wrong of a personal character resulting in injury to the feelings . . . . The injury is mental and subjective."); Crump v. Beckley Newspapers, Inc., 320 S.E.2d 70, 85 (W. Va. 1984) ("The right has primarily served to prevent . . . emotional harm").

<sup>58.</sup> See generally, Halpern, supra note 41. "In a media saturated world contemplating a future in which 'everyone will be world-famous for fifteen minutes,' the question becomes not whether a bruised soul is important but whether we can afford, and practically provide to it, the legal balm the bruise requires." Id. at 549 (quoting Andy Warhol in J. BARTLETT, FAMILIAR QUOTATIONS 908 (15th ed. 1980). Cf. Simitis, supra note 19:

Id. at 731-32 (footnote omitted).

<sup>59.</sup> Thus, the Restatement of Torts excludes from a privacy claim, matters "of legitimate concern to the public." RESTATEMENT (SECOND) OF TORTS § 652D (1977).

vacy was so limited.<sup>60</sup> Professor Post suggests "a normative theory of public accountability, on the notion that the public *should* be entitled to inquire freely into the significance of public persons and events, and that this entitlement is so powerful that it overrides individual claims to the maintenance of information preserves."<sup>61</sup>

In any event, the United States Supreme Court, in Cox Broad-casting Corp. v. Cohn, 62 and Florida Star v. B.J.F., 63 has made clear the constitutional underpinning for the newsworthiness limitation on privacy claims. 64 The Court explicitly recognized "that however it may be ultimately defined, there is a zone of privacy surrounding every individual,"65 and refused an invitation to "hold that truthful publication is automatically constitutionally protected."66 Nevertheless the Court severely limited, if it did not altogether obliterate privacy claims arising out of the publication of matter, however personal, that is derived from some kind of public record; as Justice White, the author of the Cox Broadcasting opinion, observed in dissent in Florida Star, "the Court accepts [an] invitation . . . to obliterate one of the most note-worthy legal inventions of the 20th Century: the tort of the publication of private facts."67 Certainly, the Court "seems to leave little vitality in the tort of disclosure of private facts."68

### B. IVHS and the Privacy Tort

There is thus little room for application of the paradigmatic privacy tort to the observation, capture and use of information about individuals, as contemplated in IVHS technology. The observation, individual "tagging" of automobiles which may readily be identified with individuals, would not itself appear to implicate any aspect of the privacy tort. To the limited extent that such activity—observation per se, absent publication—has been deemed actionable, it has been sur-

<sup>60.</sup> See Warren & Brandeis, supra note 40, at 214-15. ("The design of the law [of privacy] must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity") (emphasis in original). See also Post, supra note 50, at 996 ("Long before the Constitution was relevant to the regulation of the invasion of privacy tort, the common law was sensitive to just such policy concerns regarding the diffusion of information") (footnote omitted).

<sup>61.</sup> Post, supra note 50, at 1001 (emphasis in original).

<sup>62. 420</sup> U.S. 469 (1975).

<sup>63. 491</sup> U.S. 524 (1989).

<sup>64.</sup> The Court, in each case, invalidated state privacy claims arising out of the publication of offensive and embarrassing material.

<sup>65.</sup> Cox Broadcasting, 420 U.S. at 487 (emphasis in original).

<sup>66.</sup> Florida Star, 491 U.S. at 541.

<sup>67.</sup> Id. at 550 (White, J., dissenting).

<sup>68.</sup> David Anderson, Tortious Speech, 47 WASH. & LEE L. Rev. 71, 90 (1990).

reptitious and offensively intrusive.<sup>69</sup> It would be difficult to extend to an individual the right to prevent observation arising from detection devices which the individual knows are installed in his or her car. One should not, of course, emphasize too strongly the aspect of voluntariness with respect to the installation of devices in an automobile.<sup>70</sup> Although I may "voluntarily" purchase a car with knowledge of the device's presence, after the full implementation of IVHS it would in all likelihood be impossible for me to get a car without the device. Indeed, for the systems to be truly effective in dealing with traffic movement, safety, direction, and the general purposes to be achieved by IVHS, participation would have to be virtually universal. Nevertheless, the very extent of the "surveillance," the vast size of the enterprise and its lack of direct individual focus would in all likelihood preclude individual claims predicated on the intrusive nature of the activity.

So, too, with respect to the accumulation and dissemination of data—the creation and exploitation of an individual profile—the privacy tort paradigm seems inapplicable. As discussed above, the tort is at its heart founded on mass publication; the subjective, emotional interest involved arises from the violation of anonymity attendant to public exposure. The absence of any "publication" would preclude actionability of the collection process. As to dissemination, even assuming that the governmental involvement would not make the data "public" and constitutionally protect its "publication," it is not likely that the data would be subject to the kind of public exposure upon which an action must be predicated. The data would even if the publication

<sup>69.</sup> See, e.g., Nader v. General Motors Corp., 255 N.E.2d 765 (N.Y. 1970); RESTATEMENT (SECOND) OF TORTS § 652B.

Voluntarily disclosed personal information will be outside the scope of this right. Even if information is not voluntarily revealed, the particular means used to collect personal information must be highly offensive. Surreptitious or secret collections of personal information without notice or consent may be considered harmful by individuals, yet not rise to a sufficiently 'objectionable' level to meet the threshold standard.

Reidenberg, supra note 31, at 223 (footnotes omitted). See generally, Richard C. Turkington, George B. Trubow, Anita L. Allen, Privacy, Cases and Materials, Ch.2, E (1992).

<sup>70.</sup> Cf. IVHS Architecture, supra note 1, at 33 and 46, in which two of the architectural development teams suggest the absence of any privacy concerns because of acceptance by the owner/driver of the identifying devices or because "[t]here is no mandatory participation required of any citizen with respect to his or her privacy."

<sup>71.</sup> RESTATEMENT (SECOND) OF TORTS § 652D cmt. a; see supra text accompanying notes 55-57.

<sup>72.</sup> See Reidenberg, supra note 31, at 223-24:

Personal information voluntarily disclosed or available from public sources does not benefit from this [public disclosure tort] protection. As a result, activities such as the preparation and dissemination of intimate personal profiles from disparate

hurdle were overcome, it is questionable whether the "private facts" involved are such as to support a privacy claim. It may well be that my "inviolate personality" can be found in the accumulation of the ordinary, banal facts of my life—my quotidian comings and goings—but however useful such insight into my soul may be commercially, it is not the stuff of which the classic privacy tort is made.<sup>73</sup>

Information, coherently presented, has value. With the ability to gather and manipulate large amounts of data has come the "commodification" of information.<sup>74</sup> To the extent that information peculiar to me is used to further another's commercial purposes I am being commercially exploited.<sup>75</sup> However, the fact of exploitation—the eager market for screened or product-specific mailing lists is but the most obvious example—does not necessarily lead to a claim against the exploiter.

public sources of information or public revelations of information would not be actionable. Recovery under this right further requires that there be a dissemination of qualifying personal information to the general public. This is interpreted to mean general distribution to the public such as the circulation of a newspaper and not just circulation of personal information among a closed group of people.

(footnotes omitted). See also Trubow, supra note 11, at 537:

'A relatively widespread publication of the information is required to constitute an invasion of the privacy interest [and] the courts routinely accept such a limitation. Because the "publication" of commercial data maintained in computer data bases is routinely made to a small group, often one at a time, it may not satisfy this requirement.

#### 73. See Trubow, supra note 11:

Another pervasive problem in applying the private fact tort is the requirement that the information disclosed be highly offensive to a reasonable person. The courts frequently deny the tort's application when the information, though private and perhaps not of public interest, is not in itself deemed harmful or offensive. Most of the information stored in commercial computer files is not offensive or embarrassing, even though it does provide a detailed description of an individual's behavior, tastes, and values.

#### Id. at 537 (footnote omitted).

#### 74. See, e.g., Agre, supra note 14, at 120:

Regardless of its particular content, captured information is distinguished by its dual relationship—both product and representation—to the human activities upon which particular grammars of action have been imposed. In particular, the capture process makes "visible" a great deal of information-creating activity which had formerly been left implicit in the production of other, historically prior commodities. Moreover, the phenomenon of capture extends market relations not simply through the commodification of the captured information itself (if in fact that information is marketed), but also through the movement toward market relations, through a reduction in transaction costs, of the human activities that the information represents. In other words, by imposing a mathematically precise form upon previously unformalized activities, capture standardizes those activities and their component elements and thereby prepares them (again, other things being equal) for an eventual transition to market-based relationships.

#### 75. See Miller, supra note 11.

Certainly, there is a well-recognized cause of action for commercial appropriation of name or likeness.<sup>76</sup> It has been suggested that

the tort "appropriation of name or likeness" for a commercial purpose could provide an appropriate remedy [for the commercial use of computer generated information]. A compelling argument can be made that a collection of personal information sold as a dossier or profile violates the appropriation tort.... When this tort is alleged, in most instances, the appropriation has been accomplished by associating the plaintiff's personality with an advertisement for the sale of goods or services or to link him with a particular cause or viewpoint. When dossiers and profiles maintained by credit bureaus and other such agencies are sold, the subject's personality is certainly being used for a commercial purpose.<sup>77</sup>

Even here, however, adequate privacy protection is illusory. The "commercial appropriation" privacy claim need not involve offensive or embarrassing material; it is concerned simply with the commercial use of one's name or likeness. Nevertheless, as developed both legislatively and by the courts, since the interest remains the subjective interest in anonymity, freedom from *public* exposure, it would be difficult to use this vehicle to prevent the inclusion of an individual's name on a commercially available mailing list. Although the necessity for the element of widespread, public exposure has been questioned, for the extent that a claim is based upon violation of anonymity, injury to feelings, as opposed to economic harm, the privacy construct would appear to require public exposure.

<sup>76.</sup> RESTATEMENT (SECOND) OF TORTS § 652C (1977).

<sup>77.</sup> Trubow, supra note 11, at 538.

<sup>78.</sup> See infra, text accompanying notes 88-101 for discussion of the proprietary, as opposed to emotional interest in connection with commercial appropriation. Although Dean Prosser appears to equate the privacy interest here with the clearly proprietary interest implicated by the right of publicity (Prosser, supra note 46, at 406), there is a significant difference in the nature of the respective interests when one is complaining of the subjective harm, the injury to feelings that follows from an unwanted public association of one's name or likeness with a commercial endeavor and the economic injury which follows from uncompensated exploitation of the economic value of persona. See, e.g., Cohen v. Herbal Concepts, Inc., 472 N.E.2d 307 (N.Y. 1984). As the Sixth Circuit observed, "the right of privacy and the right of publicity protect fundamentally different interests and must be analyzed separately." Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831, 835 (6th Cir. 1983).

<sup>79.</sup> See Trubow, supra note 11, at 539; see also Restatement (Second) of Torts  $\S$  652C, cmt. a.

<sup>80.</sup> There does not appear to be significant case support for the RESTATEMENT OF TORTS position. The RESTATEMENT, the product primarily of Dean Prosser's approach to privacy, does not adequately deal with the personal and proprietary distinctions that can arise in the case of appropriation of identity. On the other hand, the newly adopted RESTATEMENT (THIRD) OF THE LAW OF UNFAIR COMPETITION § 46 (1993) (set out, as of this writing, in Tentative Draft No. 4, approved by the membership in May, 1993) clearly separates the economic, proprietary tort from privacy considerations.

Moreover, a *privacy* claim, as opposed to a property-based claim, <sup>81</sup> must be predicated on the use of an individual's "name or likeness" (or similar statutory formula). <sup>82</sup> Thus, even if one agrees that with respect to the kinds of uses to which IVHS information on individual activities may be put "the subject's personality is . . . being used for a commercial purpose," <sup>83</sup> that observation only begins the privacy inquiry; it doesn't resolve it. Whether the use of information as such, in the form of a data profile, is or should be actionable is a matter, as discussed below, <sup>84</sup> different from the applicability of the traditional privacy tort to this activity. It seems clear that a "profile," a data set per se, would not be a taking within the contemplation of the privacy tort. <sup>85</sup> The privacy formulation does not protect *personality* in general but only when it is appropriated by the specific identifiers.

Further, it is arguable at least that this kind of "personality profile," inherently pedestrian and unremarkable, does not amount to the unequivocal identifier of the persona that could be equated with "name or likeness." In this context, it is likely that many individuals would share the same "profile". Indeed, that very sharing is what gives a collection of such profiles (e.g., in a mailing list) its value: there is identified a discrete group of people sharing a set of traits or behavior of interest to some commercial enterprise; one individual's name, standing alone, has no real value. Does attaching a name to the profile change the calculus of rights? The name here is essentially incidental to the data set and it is at least arguable that, apart from the other impediments, the incidental character of the use would present a further obstacle to a privacy claim. 86

The narrative of an individual's life, standing alone, lacks the value of a name or likeness that the misappropriation tort protects. Unlike the goodwill associated with one's name or likeness, the facts of an individual's life possess no intrinsic value that will deteriorate with repeated use.

Id., at 438. But cf. Trubow, supra note 11, who suggests that "it is the individual's persona that is the subject of the use, and the appropriation tort ought to apply." Id. at 539.

86. See RESTATEMENT (SECOND) OF TORTS § 652C, cmt. d (1977):

No one has the right to object merely because his name or his appearance is brought before the public, since neither is in any way a private matter and both are open to public observation. It is only when the publicity is given for the purpose of appropriating to the defendant's benefit the commercial or other values associated with the name or likeness that the right of privacy is invaded.

See University of Notre Dame du Lac v. Twentieth Century Fox, 256 N.Y.S.2d 301, aff'd. 207 N.E.2d 508 (1965); see also Matthews v. Wozencraft, 15 F.3d 432, 437 (5th Cir. 1994) ("The

<sup>81.</sup> See infra text accompanying notes 88-101.

<sup>82.</sup> See, HALPERN, supra note 55.

<sup>83.</sup> Trubow, supra note 11, at 538.

<sup>84.</sup> Infra text accompanying notes 102-116.

<sup>85.</sup> See, e.g., Matthews v. Wozencraft, 15 F.3d 432 (5th Cir. 1994).

Finally, even if it were possible to fit the use of IVHS information into the privacy "appropriation" claim, protection would be limited to commercial use and would not at all extend to the matters of accumulation of data and access to it.<sup>87</sup> In short, the traditional right of privacy tort has little, if any meaningful application to the privacy issues presented by IVHS, or, indeed to the general privacy problems arising from the compilation of personal information.

## C. Proprietary Interests

Related to, but distinct from, the subjective, feelings-based privacy right, are the economic rights, in the nature of proprietary rights. that an individual may have in matters concerning him or her self. The "right of publicity" has grown and matured in the law as the means for protecting the economic, associative value of persona from commercial exploitation.88 The right of publicity as currently understood was the product of the determination of the Second Circuit in Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc. 89 recognizing a cause of action for damages and other relief for the unauthorized commercial appropriation of an individual's persona based upon the economic value of the persona and independent of a common-law or statutory right of privacy. Haelan was the start of a judicial and legislative movement delineating an economic right in one's persona distinct from the right of privacy. The linkage of the economic interest in personality with the privacy interest in solitude, the right to be free from public exposure, has been the source of much confusion.<sup>90</sup> After forty

[I]t is possible that [the appropriation] right could apply to ban certain uses, including dissemination, of personal information for commercial purposes without consent. However, privacy concerns associated with the collection of personal information—notice and consent to data acquisition, unnecessary data compilation, and accuracy of data—and the storage of personal information would be outside the scope of this misappropriation right.

misappropriation tort does not protect one's name per se; rather, it protects the value associated with that name").

<sup>87.</sup> See Reidenberg, supra note 31, at 225:

<sup>88.</sup> For a comprehensive examination of the right of publicity, its relation to the other interests and a detailed examination of the state and federal, common-law and statutory treatment of the subject, see generally McCarthy, supra note 38; see also Halpern, supra note 48, Part Three—Publicity; Sheldon W. Halpern, The Right of Publicity: Commercial Exploitation of the Associative Value of Personality, 39 Vand. L. Rev. 1199 (1986).

<sup>89. 202</sup> F.2d 866 (2d Cir.), cert. denied, 346 U.S. 816 (1953).

<sup>90.</sup> See, e.g., Richard C. Ausness, The Right of Publicity: A 'Haystack in a Hurricane,' 55 Temp. L.Q. 977, 981-83 (1982); Tim Frazer, Appropriation of Personality—A New Tort?, 99 LAW Q. Rev. 281, 295-99 (1983); Andrew B. Sims, Right of Publicity: Survivability Reconsidered, 49 Fordham L. Rev. 453, 464-65 (1981); David E. Shipley, Publicity Never Dies; It Just Fades Away: The Right of Publicity and Federal Preemption, 66 Cornell L. Rev. 673, 681-82 (1981).

years of maturation, the independent economic right seems to be firmly established.<sup>91</sup> The new *Third Restatement of the Law of Unfair Competition* clearly separates the economic, proprietary tort from privacy considerations:

Appropriation of the Commercial Value of a Person's Identity: The Right of Publicity

One who appropriates the commercial value of a person's identity by using without consent the person's name, likeness, or other indicia of identity for purposes of trade is subject to liability for [monetary and injunctive] relief.<sup>92</sup>

Here the right has fully emerged, free of its analogic ancestors, free of the constraints of a privacy pigeonhole in the *Restatement of Torts*. With a base in the law of unfair competition, the commercial, economic, appropriation characteristics of the interest to which the right of publicity relates are fully recognized.

Of course, as with the "appropriation" right of privacy, this right has no application to the collection, compilation and storage of data; it is limited to commercial appropriation of identity. As to the commercial taking, the independent right of publicity is not limited to the privacy "name or likeness" formulation but should be applicable to the taking of identity by whatever means serve to effectuate that taking.

In most cases the appropriation of identity is accomplished through the use of a person's name or likeness.... In the absence of a narrower statutory definition, unauthorized use of other indicia of a person's identity can also infringe the right of publicity... if they are so closely identified with the person that their use enables the defendant to appropriate the commercial value of the person's identity.<sup>93</sup>

Thus, if one could demonstrate that a personality profile is indeed an unequivocal identifier of a given individual,<sup>94</sup> then presumably the

<sup>91.</sup> See Michael Madow, Private Ownership of Public Image: Popular Culture and Publicity Rights, 81 Calif. L. Rev. 125, 133 (1993) ("Most courts accept the existence of the right and concern themselves with polishing its contours"); McCarthy, supra note 38, at § 1.10[C]. There are, of course exceptions, the most prominent of which is the determination by the New York Court of Appeals rejecting a common-law right of publicity independent of New York's statutory right of privacy. Stephano v. News Group Publications, Inc., 474 N.E.2d 580, (N.Y. 1984).

<sup>92.</sup> RESTATEMENT (THIRD) OF THE LAW OF UNFAIR COMPETITION § 46 (1993).

<sup>93.</sup> Id., cmt. d. See Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831, 835 (6th Cir. 1983) ("If the celebrity's identity is commercially exploited, there has been an invasion of his right whether or not his 'name or likeness' is used"); Midler v. Ford Motor Co., 849 F.2d 460 (1988), cert. denied, 112 S. Ct. 1513 (1992); Waits v. Frito-Lay, Inc., 978 F.2d 1093 (9th Circ. 1992).

<sup>94.</sup> But see supra text accompanying notes 85-86.

right of publicity would be implicated by the commercial taking of the profile, and the issue of whether the use of name in that context is merely "incidental" would be moot.

However, there remain serious obstacles to application of the right of publicity to the commercial use of personal data. The right of publicity has been peculiarly celebrity based; it has been concerned with commercial appropriation of the associative value of personality. Finally 196 In that sense it has focused on the fact common to the cases that the association with a well known person has served to enhance the economic value of a product. There is certainly scholarly dispute over the necessity of celebrity as an element of the right of publicity claim, and the Third Restatement of Unfair Competition suggests that there is no such limitation. Nevertheless the cases—and the right is essentially a common-law right—have been almost exclusively concerned with appropriation of the associative value of a celebrity, one whose identity has commercial value by itself.

In any event, again, as with the privacy-based "appropriation" claim, even if the claim could be extended to the non-publication, private transactional uses contemplated in IVHS, the scope of protection afforded by a right of publicity claim would be far narrower than the array of privacy concerns raised by IVHS.

<sup>95.</sup> See supra note 86 and accompanying text.

<sup>96. &</sup>quot;At its heart, the value of the right of publicity is associational." McFarland v. Miller, 14 F.3d 912, 919 (3d Cir. 1994). "Its primary purpose is to protect public figures and to provide them with a descendible and assignable right." Trubow, *supra* note 11, at 538.

<sup>97.</sup> See Frazer, supra note 90, at 308; Richard B. Hoffman, The Right of Publicity—Heir's Right, Advertisers' Windfall, or Courts' Nightmare?, 31 DE PAUL L. REV. 1, 5 (1981); Andrew B. Sims, Right of Publicity: Survivability Reconsidered, 49 Fordham L. Rev. 453, 473 (1981). But, cf., Harold Gordon, Right of Property in Name, likeness, Personality and History, 55 NW. U.L. Rev. 553, 554-55 (1960); Roberta R. Kwall, Is Independence Day Dawning for the Right of Publicity?, 17 U.C.D. L. Rev. 191, 202-03 (1983) (advocating recognition of a 'universal' right of publicity); Melville B. Nimmer, The Right of Publicity, 19 LAW & CONTEMP. PROBS. 203, 204 (1954); Harriet Pilpel, The Right of Publicity, 27 BULL. COPYRIGHT SOC'Y 249, 255-56 (1980); Shipley, supra note 90, at 723-24 n.325 (1981).

<sup>98. &</sup>quot;[C]elebrities are not precluded from establishing cognizable injury to personal interests in addition to commercial loss, nor are less well-known plaintiffs precluded from establishing commercial loss in addition to injury to personal interests." RESTATEMENT (THIRD) OF THE LAW OF UNFAIR COMPETITION § 46 cmt. a. (1993).

<sup>99.</sup> See, e.g., Martin Luther King, Jr., Center for Social Change, Inc., v. American Heritage Prods., Inc., 296 S.E. 2d 697, 702 (Ga. 1982); Matthews v. Wozencraft, 15 F.3d 432, 438, n.2 (5th Cir. 1994) ("We grant celebrities a property right to ration the use of their names in order to maximize their value over time"); McFarland v. Miller, 14 F.3d 912, 919 (3d Cir. 1994) ("[a] famous individual's name, likeness, and endorsement carry value and an unauthorized use harms the person both by diluting the value of the name and depriving that individual of compensation"); Ali v. Playgirl, 447 F. Supp. 723 (S.D.N.Y. 1978) ("The distinctive aspect of the common law right of publicity is that it recognizes the commercial value of the . . . representation of a prominent person or performer, and protects his proprietary interest in the profitability of his public . . . 'persona' "). See generally Halpern, supra note 88.

In short, just as with the classic right to privacy complex, it is difficult to find proprietary concepts that adequately address the privacy concerns raised by information technology. My life may be "mine," but I don't necessarily have a property interest in its minutia. The facts of one's life, the things we do that may help to define us, are not themselves within the ambit of protection to be found in the right of publicity; nor are they the stuff of copyright or similar intellectual property concepts. If the individual is to have meaningful control over the collection, compilation and use of observed personal data, that control must come from a legal construct specifically created for that purpose. That construct must peculiarly address the problem of "informational privacy," divorced from the classic privacy or property concepts underlying existing law. Io2

#### IV. INFORMATIONAL PRIVACY

There is a growing body of literature attempting to define and expand upon the right to control and limit access to personal information through a "legal right to informational privacy," and it is not the purpose of this essay to redundantly survey the field. What has emerged clearly is that "[i]n the United States . . . no single source of privacy rights covers each data processing activity. Information privacy rights emerge from a complex web of federal and state laws that have responded to narrowly identified problems . . . ." 104

At the federal level, such privacy protection as exists is diffuse and uncoordinated. <sup>105</sup> There is, most prominently, the federal statutory informational privacy rights concerned primarily with access to and

<sup>100.</sup> Consider Who Owns a Life? Asks a Poet, When His Is Turned Into Fiction, N.Y. TIMES, Feb. 20, 1994, Sec. 4, at 14, c. 1.

<sup>101. &</sup>quot;[N]o author may copyright facts or ideas." Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 547 (1985). See Hoehling v. Universal City Studios, Inc., 618 F.2d 972 (2d Cir. 1980); Nash v. CBS, Inc., 899 F.2d 1537 (7th Cir. 1990); Narell v. Freeman, 872 F.2d 907 (9th Cir. 1989).

<sup>102.</sup> See Note, supra note 22, at 1413:

<sup>[</sup>C]ourts have usually rejected claims based on information privacy. The few reported cases reflect the difficulty of making claims of violating information privacy. Plaintiffs and courts have attempted to squeeze these claims into the existing framework of privacy law instead of recognizing that a new cause of action is needed in the information age.

<sup>103.</sup> Turkington, supra note 39, at 487. See generally, Turkington, id.; Trubow, supra note 11; Reidenberg, supra note 31; Simitis, supra note 19; Note, supra note 22; see also Turkington, Trubow, and Allen, supra note 69, Ch. Two—Informational Privacy.

<sup>104.</sup> Reidenberg, supra note 31, at 201. For discussion of informational privacy legislation in Europe, see id. at 200-201, and Simitis, supra note 19, passim.

<sup>105.</sup> See Trubow, supra note 11, at 530 ("no single federal agency is vested with the overall responsibility of safeguarding informational privacy with respect to federal records [and] no provision exists for the coordination of privacy policy throughout the federal establishment").

use of governmentally collected data. Thus, the Privacy Act of 1974<sup>107</sup> is designed to prevent federal agencies from disclosing certain personal information contained in agency records. Similarly, the Freedom of Information Act contains limitations on disclosure of agency information when such disclosure would constitute a "clearly unwarranted invasion of personal privacy." There are also industry-specific laws, federal and state, <sup>109</sup> that "provide a sphere of protection to isolated concerns for narrowly-identified problems and are incomplete responses to information privacy issues. This ad hoc . . . approach leaves many areas of information processing unaddressed . . ."<sup>110</sup> While parts of this body of legislation might be useful in structuring the IVHS, <sup>111</sup> they do not provide a coherent and consistent means of balancing the personal privacy needs of the individual involved in the system with the broad societal goals of safety, efficiency and convenience to which IVHS is directed.

Adequate recognition of informational privacy in general, in the various contexts in which the issue arises—crossing conceptual, technological and political boundaries—will not be found either in procrustean manipulation of the common law of privacy or in an incoherent complex of disparate special purpose legislation. If privacy considerations were the only criterion, then a comprehensive federal<sup>112</sup> legislative scheme directed to the collection, compilation,

The scope of protection accorded by each of these industry-specific laws is generally limited. The full range of issues with respect to data processing activities for personal information, such as fairness in the collection of data, data minimization, data accuracy and permissible use of personal information, are not consistently treated at the federal level.

Id at 210.

Because personal information flows are not confined to state or national borders, it may be most appropriate to adopt any new rights at the federal level. Differences in privacy protection among the states could readily have adverse or distorting effects on interstate commerce and international data flows. Business has

<sup>106.</sup> For discussion and review of the various federal statutes see Turkington, Trubow, AND ALLEN, supra note 69, at 331-79.

<sup>107. 5</sup> U.S.C. § 552a (1988).

<sup>108. 5</sup> U.S.C. § 552(b)(6) (Exemption 6). See United States Department of Defense v. Federal Labor Relations Authority, 114 S. Ct. 1006 (1994), in which the Court gave a broad reading to the limitation, building on United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 765 (1989).

<sup>109.</sup> Reidenberg, supra note 31, at 209-20, 229-34. As Reidenberg notes:

<sup>110.</sup> Id. at 209-10.

<sup>111.</sup> E.g., The Cable Communications Policy Act creates an array of rights for cable subscribers and limitations on how a cable system may collect and store subscriber information and what it may do with that information. 47 U.S.C. § 551(a)(1) (1988).

<sup>112.</sup> The trans-boundary nature of much of the technology that feeds personal information databases would probably be sufficient itself to provide the foundation for comprehensive federal preemptive intervention.

storage, access to and dissemination of personal information would be the optimal means of providing a coherent and effective informational privacy blanket around information technology. While there is undoubted appeal in such comprehensive coverage, there is also serious question about the desirability of such a blanket.

Generalization about informational privacy is dangerous. "[S]ocial discourse depends on an information allocation policy that, through a mix of withholding and access, reflects a precise analysis and understanding of the consequences of automated processing for both the individual and society." Information, as such, compiled and correlated collections of data, is neither good nor evil; the technology, developed and developing, for the collection and manipulation of data offers the potential for social good and the opportunity for oppressive abuse 114 and any policy relating to the limitation of access and use of technologically generated information must in a sophisticated manner consider all of the interests and preserve as much of the good as is consistent with societal health.

[T]he boundary between a permissible exchange of facts about people, necessary to avoid misrepresentation, and an impermissible intrusion and surveillance is entirely unclear. . . . The answer depends essentially on the particular purposes of each data collection as well as on the mode of the information process and the potential implications of the data use for the persons under scrutiny. 115

While we speak of "informational privacy" in general terms, the issue arises in highly specific situations in which there is a continual need to balance the individual privacy needs and the overall societal information needs. Limitation and restriction in one area (e.g., maintenance of individual credit card purchase information for targeted mailing lists) may be singularly inappropriate in another (e.g., general credit history for credit granting purposes); similarly, the kinds of lim-

historically supported uniformity of any mandatory rules to avoid the confusion of fifty separate sets of state privacy regulations.

Reidenberg, supra note 31, at 238-39 (footnotes omitted).

<sup>113.</sup> Simitis, supra note 19, at 735 (footnote omitted).

<sup>114. &</sup>quot;[T]he processing of personal information . . . in a great number of situations in the public as well as the private sector serves both the user and the individual under scrutiny." *Id.* at 739.

<sup>115.</sup> Id. at 709 (footnote omitted).

The increased access to personal information resulting from modern, sophisticated techniques of automated processing has sharpened the need to abandon the search for a 'neutral' concept in favor of an understanding free of abstractions and fully aware of the political and societal background of all privacy debates.

itations considered essential on governmental agency activity may well be unnecessarily restrictive when applied to a specific private industry. In short, it may be necessary to continue to deal with specific information privacy issues in a piecemeal fashion. A comprehensive informational privacy legislative blanket suffers from the debility either of being too general, too thin to be of any real value, or of being too specific and inflexible to foster rather than stifle necessary and productive information technology.<sup>116</sup>

# V. PRIVACY AND IVHS: A MINIMALIST TECHNOLOGICAL ACCOMMODATION

Technical resources . . . must be mobilized. Instead of a simple focus on the convenience of the potential user, the safeguarding of privacy must become an equally powerful consideration in all further development of information technology. Hardware and software should, like motor vehicles or medicine, meet certain safety requirements before being put on the market. They should have a minimum of built-in protective devices. This requirement is by no means a utopian expectation. 117

If we deal specifically with the privacy issues raised by IVHS, rather than seek a broad informational privacy legal paradigm, a workable accommodation of the conflicting interests may be feasible. By looking at the purposes of IVHS, the specific uses to which the technology is to be put—rather than the uses which may arise from the existence of the technology once in place—the systems may be designed both to facilitate accomplishing their purposes and to minimize interference with personal privacy. The technology itself, through the system architecture, can be the vehicle for accommodation.

Thus, while concern over the "dossier" and its use can be somewhat alleviated by means of carefully crafted restrictions on access and on dissemination and commercial use, 118 in the context of IVHS a

<sup>116.</sup> Cf. Reidenberg, supra note 31, at 238-43.

While the public interest suggests that an articulated set of legal rights respond systematically to the plethora of privacy concerns, a purely general approach is likely to lead to difficulties balancing individual and commercial interests. Some means to accommodate both varying contexts for the processing of personal information and varying levels of concern may be necessary.

Id. at 240. Reidenberg discusses the European experience (Id. at 237-41) and notes that "[t]he trend in more recent European national legislation also recognizes the complexity of the information economy and the need for greater flexibility." Id. at 241.

<sup>117.</sup> Simitis, supra note 19, at 739.

<sup>118.</sup> In short, a scheme of tailored regulation that inevitably would entail the need to build in exceptions and invite the search for exploitable lacunae.

more promising avenue is in the collection/storage process itself. None of the IVHS goals require more than transitory retention of personal data. While a given system is operating—its real time functioning—it may be necessary specifically to identify a tagged vehicle, but the purpose of the system is not furthered by retention of the identifying tags themselves. Advanced Vehicle Control systems, directed to individual, specific vehicles, need to identify the vehicle, but only so long as the system is operating on that vehicle; similarly, the Automatic Vehicle Identification, Automatic Vehicle Location, Advanced Traveler Information Systems, and other systems designed to assist or provide information to individually identified vehicles need the identification only for the immediate action taken. Even for the mundane matter of toll collection, the use of "smart cards" does not require user identification or the maintenance of individual accounts if users simply use pre-purchased, "bearer" cards which exhaust their value as they are used at collection or tracking stations. 119

Retention of individually identified behavioral data or other vehicle specific information as such then is extraneous to the system's ends, however ultimately useful for other purposes or exploitable it may be. The IVHS mandate<sup>120</sup> is transportation-specific. The purpose of IVHS is "to help... in meeting the goals of ISTEA,"<sup>121</sup> the Intermodal Surface Transportation Efficiency Act of 1991.<sup>122</sup> ["T]he emphasis [of IVHS is] on enhancing the existing transportation system."<sup>123</sup> Deployment of IVHS is seen as "leading to safety improvements, amelioration of congestion, reduced environmental impact, more efficient energy use, and enhanced national productivity."<sup>124</sup> Information data banks *per se* are not part of this vision.

If technological restriction is placed on retention of individually identifiable data, issues of profile creation or commercial exploitation of name and history become academic; IVHS is lifted bodily outside the informational privacy debate. While one may view built in technological restriction as a ways of limiting the potential of the technology, the aim of IVHS is not technology for its own sake but its application to specific transportation needs. Rather than disabling, restricting collection is a form of technological parsimony—using technical skill and resources to meet specific important societal needs. "Some . . .

<sup>119. &</sup>quot;Smart cards and videotex can, at least for payment purposes, be designed in a way that demands almost no collection of personal data," Simitis, *supra* note 19, at 740.

<sup>120. 23</sup> U.S.C. § 307 nt.

<sup>121.</sup> STRATEGIC PLAN, supra note 5, at I-2.

<sup>122. 49</sup> U.S.C. § 101 nt.

<sup>123.</sup> Williams, supra note 4, at 683.

<sup>124.</sup> STRATEGIC PLAN, supra note 5, at II-1.

privacy concerns may be resolved through the use of technology..... Information networks may be structured to provide only the minimal amount of personal information necessary to accomplish a particular task and to delete personal information as soon as it is no longer needed."<sup>125</sup>

In short, what is suggested is that the informational privacy problems be addressed at the level of system architecture. Consistent with the purposes underlying IVHS, the component systems can be designed to avoid the collection of personally identifiable data except where necessary to system functioning and, in those instances, to provide for the purging of tags and other individually referable references once the immediate need for the identification has passed. In view of the deep federal involvement, the federal legislative foundation for the development of the systems, and the obvious nationwide scope of the undertaking, federal legislation with respect to this aspect of system architecture would be perfectly appropriate. In an application of Occam's Razor, the technology out of which the problem arises becomes the vehicle for its solution.

#### VI. Conclusion

The "classic" privacy tort, both in its teleology and in the way it is currently applied, has little significant application to the issues of observation, data collection, storage, access, dissemination and use which make up the IVHS privacy complex. Similarly, the proprietary interests which underlie the rights of publicity and intellectual property, are not directed to the data and uses that impact upon individual privacy through this technology. The issues here, essentially those of "informational privacy," cannot be dealt with by the existing common law without serious distortion of both the law and the interests to be protected. Nor do existing informational privacy statutes provide appropriate protection that is consistent with the aims to be achieved by IVHS. Technological variety and the multi-faceted character of data collection and manipulation in diverse contexts would appear to preclude seeking comprehensive federal legislation to deal with informational privacy and technology in general, that would, inter alia,

<sup>125.</sup> Reidenberg, supra note 31, at 239-40.

<sup>126.</sup> A cognate issue arose in connection with copyright protection for musical recordings following the development of consumer directed digital audio tape equipment. Such equipment can be used to make digital recordings of audio compact disks ostensibly indistinguishable in quality from the original. Driven by fear of widespread infringement, musical copyright owners sought to prevent importation of these devices. Ultimately, the problem was resolved for all practical purposes by legislation requiring such equipment to be so constructed as to prevent making of serial digital copies (i.e. copies of copies) of a digital original. See 17 U.S.C. § 1001.

embrace the IVHS privacy concerns. Rather, what is appropriate in the context of the Intelligent Vehicle Highway Systems—where little purpose is served by the retention of personal data—is limited, tightly tailored restrictions on the technology itself, sharply constricting the ability of the systems to retain personal data. Ultimately, even if only through general guidelines, the overall problem of informational privacy in a high technology, information oriented society, will have to be faced. The IVHS presents neither the appropriate problem nor is it the appropriate vehicle for such an endeavor.

