Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 11 | Issue 1 Article 10

January 1995

Reasoning About the Future: The Technology and Institutions of Intelligent Transportation Systems

Philip E. Agre

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

 Part of the Law Commons

Recommended Citation

Philip E. Agre, *Reasoning About the Future: The Technology and Institutions of Intelligent Transportation Systems*, 11 Santa Clara High Tech. L.J. 129 (1995).
Available at: http://digitalcommons.law.scu.edu/chtlj/vol11/iss1/10

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.

COMMENT

REASONING ABOUT THE FUTURE: THE TECHNOLOGY AND INSTITUTIONS OF INTELLIGENT TRANSPORTATION SYSTEMS

Philip E. Agre†

I. INTRODUCTION

A debate about Intelligent Transportation Systems (ITS) is not simply a debate about technology.[1] It is, rather, a debate about the future interactions between technologies and institutions that our choices today will set into motion. Arguments about such things are difficult to make with any reliability, and it is easy to lapse into extremes. At one extreme is an unsophisticated optimism for which the unpredictability of future events encourages us to err on the side of progress. At another extreme is an unsophisticated pessimism for which the possibilities for authoritarian misuse of information technology encourage us to regulate it out of existence. To make prudent choices about ITS, it is necessary to develop concepts that help clarify the interactions between institutions and technologies. This article will pay particular attention to the institutions of computer system design and technical standard-setting.[2]

The United States Department of Transportation and a non-profit industry group called ITS America are currently engaged in an elaborate process aimed at the creation of an "architecture" for American ITS systems.[3] This is a delicate process, driven by several considerations:

Copyright 1995 by the author

† Assistant Professor in the Department of Communication at the University of California, San Diego.

1. These systems were referred to until recently as Intelligent Vehicle-Highway Systems (IVHS).

2. For a more extended discussion of these and related issues, *see* Philip E. Agre and Christine A. Harbs, 7(3) SOCIAL CHOICE ABOUT PRIVACY: INTELLIGENT VEHICLE-HIGHWAY SYSTEMS IN THE UNITED STATES, INFORMATION TECHNOLOGY AND PEOPLE (1994), in press.

3. UNITED STATES DEPARTMENT OF TRANSPORTATION AND IVHS AMERICA, IVHS ARCHITECTURE DEV. PROGRAM INTERIM STATUS REP., Apr. 1994.

(1) ITS systems are complex. The phrase ITS actually covers a diverse group of technologies and services. Although it would be desirable for these technologies and services to be designed to common standards, various segments of the industry may acquire their own momentum independently of the others.

(2) Most U.S. roadways are controlled by state agencies, usually with the aid of Federal funding. ITS system design is thus an occasion for a complex negotiation of government and private roles in operating a significant portion of the country's infrastructure.

(3) Although as a marketing matter ITS systems need only be standardized on a continent-by-continent basis, U.S. manufacturers may find themselves competing with standards and systems currently being developed in Europe and Japan. If American ITS systems were to develop piecemeal through market selection among a welter of partially defined architectures, the time required for a single "winning" architecture to emerge might create a opening for better-coordinated foreign alternatives.[4]

(4) The major industrial firms in the ITS America alliance may have a common interest in developing a coherent American architecture, but their interests diverge in other ways. Each firm has its own distinctive strengths and styles, and the emerging architecture definition will set the terms of competition among these firms within the American market.

Clearly, then, decisions about privacy in ITS systems will be made will be made in a complicated institutional context. The stakes for these institutions are high, given uncertainty about market acceptance of the systems that will emerge from this process. Past experience with ITS provides some precedent for concern. A proposed road-pricing scheme in Hong Kong based on on Automatic Vehicle Identification (AVI) encountered considerable resistance from advisory boards and professional associations based on privacy concerns and the interpretation of road use fees as unwelcome taxation.[5] At the same time, even if ITS systems do not become legally mandatory, they may be introduced in such a way that they become a practical necessity for large parts of the population. Such a circumstance might arise, for example, through the demands of insurance coverage or because of the lengthening lines at now understaffed manual toll-paying stations.

---

4. Lawrence A. Berardinis, *Smart highways get the green light*, 64 MACHINE DESIGN (1992), at 66-70.

5. Sandford F. Borins, *Electronic road pricing: An idea whose time may never come*, A 22A(1) TRANSP. RES. (1988), at 37-44.

It is thus difficult to predict accurately, or even conceptualize clearly, the locus of "consent" for participation in ITS.

On a technological level, the key decisions about privacy in ITS revolve around a single issue, namely whether the computers in the system capture information about individual cars or drivers in individualized form — that is, in a form that is indexed by a unique identifier for either the car or driver, or by some other code that can be readily employed to cross-index multiple databases, thus constructing a dossier about a given individual. It is worth emphasizing that this is not simply a matter of data security. Significant potential dangers from ITS systems do not derive only from unauthorized access to personal information. They also derive from institutional pressures to employ this information for secondary purposes such as marketing. Government agencies are today engaged in a great deal of marketing on behalf of the businesses in their jurisdictions,[6] and ITS information could facilitate a great expansion of such activities. The proliferation of computer-mediated tracking systems for numerous categories of people (immigrants, "deadbeat dads", and so forth) is also a matter of concern, and imperatives of law enforcement will surely wear down any institutional protections for individualized ITS data. Perhaps these secondary uses of ITS data are actually part of the systems' intended functionality, in which case that fact should be openly confirmed and debated. It will be assumed here that ITS is intended solely to facilitate safety and efficiency in highway traffic.

II. COMPUTER SYSTEM DESIGN

Let us first consider the institutions of computer system design. On a technical level, it seems easy enough to pose the question of whether ITS should capture individualized information. Yet within the traditions of system design, this question can only be posed in a limited and prejudicial way. In another work,[7] I have characterized these traditions in terms of the "capture model". When a system is meant to support human activities, traditional design methods begin by fashioning an ontology — a formal system of categories and relationships to describe the people and things that populate that particular domain of activity. The next step is to embody this ontology in a representational scheme, on the assumption that technical means will be provided to "capture" the relevant aspects of the unfolding activity.

6. PHILIP KOTLER, DONALD H. HAIDER AND IRVING REIN, MARKETING PLACES: ATTRACTING INVESTMENT, INDUSTRY, AND TOURISM TO CITIES, STATES, AND NATIONS (1993).

7. Philip E. Agre, *Surveillance and Capture: Two models of privacy*, 10(2) THE INFORMATION SOCIETY (1994), at 101-127.

The logic underlying this procedure is simple enough: a computer can only compute with what it can represent, and it can only represent what it can capture. The real-time capture of individualized information — that is, information indexed by a unique identifier for each individual — is thus a wholly natural application of standard design practices. The space of design alternatives is defined in terms of restrictions upon the ontology. For example, one might eliminate identifiers for people but retain them for cars, or eliminate identifiers for cars but retain them for individual "smart cards" that might potentially be purchased anonymously. Each limitation placed upon the ontology reduces the potential functionality of the system. Designers will typically experience the resulting constraints as artificial, and they will not normally burden themselves with those constraints voluntarily.

It is not an exaggeration to say, then, that privacy invasion is an inherent tendency of the conventional practices of computer system design. Alternative technical methods do exist, particularly schemes like "digital cash" that employ cryptography to authenticate transactions. In a digital cash scheme, individual drivers would carry devices that generate "cash" (electronically encoded promises to pay certain sums) and pass these through their financial institution for validation before sending them to the service provider. Public-key cryptography assures the service provider of the integrity of the transaction without necessarily identifying the customer.[8] If ITS is to avoid capturing large amounts of individualized data, though, the necessary social decision-making process will be swimming upstream against the conventional practices and the tremendous inertia that they have developed within the institutions of computing.

III. TECHNICAL STANDARDS

Design practices are not the only source of inertia in technical choices about privacy. The typical complex technological system combines elements from a number of vendors, each of which must also function as part of numerous other systems as well. (Some exceptions to this rule are found among military systems, which are often designed with more custom and fewer off-the-shelf parts than commercial systems.) This means that standards must be defined for the interfaces among these components. The prototype of such standards might be pipe threads: pipes and elbows made by different manufacturers can be fastened together if they conform to a common standard. Standards can arise through a number of mechanisms. One

8. Eamonn Sullivan, *Firm has technology you can bank on: With "digital cash", transactions made over public networks remain secure and private*, 11(34) PC WEEK (1994), at 83-85.

source of standards is the state: telecommunications standards, for example, have historically been negotiated by governments concerned with the interoperability of national systems. Standards can also arise through negotiations among alliances of commercial firms, conducted either through professional associations or (especially in recent times) privately.[9] ITS standard-setting in the United States combines elements of all three of these mechanisms, particularly if the DOT/ITS America architecture development project is included.

But standards frequently persist through mechanisms far distant from the institutions that defined them. Regardless of the origins of pipe-thread standards, for example, a manufacturer seeking to market a new line of pipes will be well-advised to conform to the existing standard for pipe threads. Unless the new pipes are aimed at an entirely new market, they will often need to interconnect with existing pipes. Manufacturers of computer keyboards, likewise, have a powerful interest in conforming to the basic QWERTY layout. Even though demonstrably superior layouts exist, at no point is it simultaneously in the interest of enough people to convert to any other standard.[10]

The entrenchment of technical standards in the marketplace has profound consequences for ITS systems. Some of these have already been alluded to at the outset. Once a large number of systems has been deployed that operate according to certain standards, that very fact will most likely create a powerful economic interest in the perpetuation of those standards, even among companies whose products have not even been designed. Among the most fundamental of standards for the interoperability of ITS products will be the scheme employed to define users' interactions with the systems. If this scheme requires the routine capture of individualized data, then that convention will most likely become entrenched in the market. Conversely, if a scheme based on anonymous transactions becomes established then that scheme will most likely become entrenched instead.

Which of these scenarios emerges will depend on some combination of government policy, private alliance-building, market demand, and pure chance. It is entirely possible, for example, that a set of ITS standards with no privacy protection beyond simple data security will emerge haphazardly through incremental extension of existing systems originally meant for state agencies charged with regulating com-

9. William J. Drake, *Europe in the new global standardization environment, in* TELECOMMUNICATIONS IN EUROPE: CHANGING POLICIES, SERVICES AND TECHNOLOGIES (Charles Steinfield, Laurence Caby, and Johannes Bauer, eds.)(1992).

10. Paul A. David, *Clio and the economics of QWERTY*, 72(2) AM. ECON. REV. (1985), at 332-337.

mercial truck traffic. On the other hand, it is equally possible that a different set of standards might grow haphazardly around any of a number of AVI schemes based on radio-frequency "transponders" which broadcast their own internal identifier, not that of a person or car. Or else the architecture development activities being conducted by DOT and ITS America may function as intended by delivering a set of standards organized around consciously chosen principles.

IV. CULTURE AND PARTICIPATION

Though brief, this analysis of technical institutions permits a more careful framing of the crucial question: what are the conditions of informed social choice about privacy issues in ITS?

Some of these conditions are cultural. Social responses to the privacy issues raised by new technologies will presumably be conditioned by historical experiences and the symbolic encodings of historical memory. The single most important cultural understanding of privacy issues, at least in the United States, is derived from historical experiences (mostly in Europe) of the secret police. These experiences are most frequently voiced through visual metaphors (as in the term "surveillance"), and most especially through the allegorical vocabulary of Orwell's 1984 ("Big Brother is Watching You").[11] While these cultural forms encode genuine historical experiences of state oppression, they nonetheless fail to articulate adequately a variety of other threats to privacy. They are only obliquely relevant to most projected implementations of ITS, for example, in which participation is supposed to be voluntary.

"Big Brother" metaphors for technological privacy issues are accurate in one unfortunate way: in both Big Brother's world and our own, most people have little understanding of the technical and institutional machinery through which routine surveillance is implemented in daily life.[12]

It is a matter of "they know everything about us", without any very definite reference for the "they" or the "everything". This abstract understanding is unfortunate because it encourages a passive fatalism about the control of technology, as well as a diffuse and corrosive distrust of the institutions of society.

---

11. GEORGE ORWELL, 1984: A NOVEL (1949); 1984 REVISITED: TOTALITARIANISM IN OUR CENTURY, (Irving Howe, ed.)(1983).

12. CENTER FOR PUBLIC INTEREST LAW, PRIVACY RIGHTS CLEARINGHOUSE, FIRST ANNUAL REPORT OF THE PRIVACY RIGHTS CLEARINGHOUSE, University of San Diego (1993), at 11-13; H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA (1994), at 146-150.

One possible condition of informed social choice about ITS, then, is the "visibility" of the machinery of data-collection. This includes a variety of disclosure requirements, but it might also include requirements that organizations employing personal data collaborate in the publication of "maps" of the circulation of this data among various uses. Such visibility might help rectify a broad category of routine market failures by permitting individuals to make fully informed choices about the contracts they enter into — most particularly those adherence contracts which incorporate implicit or otherwise obscure terms concerning secondary uses of personal information. It might also provide the grounding in personal experience that permits people to make informed choices about political matters, including the choice to commit oneself to activism on particular issues.

The obstacles to genuine public participation in the most consequential decisions about ITS are considerable. These crucial decisions are located largely in the establishment of technical standards for the capture and exchange of transactional information. These are, unfortunately, among the earliest and most conceptually obscure decisions to be made about ITS. Moreover, they are likely to be made as part of a much larger and heavily interconnected network of decisions, now being negotiated among a large number of institutional parties. Once technical standards have become entrenched in the market, it is unlikely that they will be changed through legislative, administrative, or judicial action, or through consumer boycotts and the like. The collective impact of individuals' refusals of privacy-invasive ITS functionalities may have some effect, but such a scenario presupposes that sufficiently many individuals understand the issues and that other legal and economic pressures permit them the option of refusal as a practical matter. In any event, the economic forces for standardization make it unlikely that individuals, or even sizeable organized groups, would have an adequate bargaining position to force architectural modifications to large-scale systems that are already in place.

V. Conclusion

Lacking effective public participation in the ITS design, it is likely that the controversy will move from democratic processes into the realm of symbolic manipulation. Data security will no doubt be emphasized in place of privacy. Practicality of anonymous use of ITS will no doubt be exaggerated. Vague and dystopian "Big Brother" scenarios will continue to fill the newspapers. Nonetheless, a clear role is emerging for a new form of public activism, in which citizens versed in technical matters serve as mediators between technical deci-

sion-making and the broader public. Volunteer activists associated with a public-interest organization called Computer Professionals for Social Responsibility (CPSR), for example, have been active in shaping the privacy-related aspects of the state-mandated AVI standards in California.[13] The Internet now brings detailed information on such issues a rapidly expanding audience, and similar forms of electronic communications may facilitate more informal and participatory forms of interchange among government, industry, activists, and the broader public than is possible through existing media. As a practical matter, learning to use computer networks for such democratic ends will be a long and difficult process. The alternative, though, is a technology-driven revolution in transportation infrastructure that will materially diminish the ability of citizens to travel and associate without leaving records behind them.

13. Personal communication with author from Chris Hibbert and Lee Tien of CPSR.