



1-1-1995

Privacy and IVHS: A Diversity of Viewpoints

Margaret M. Russell

Santa Clara University School of Law, mrussell@scu.edu

Follow this and additional works at: <http://digitalcommons.law.scu.edu/facpubs>

Recommended Citation

11 *Santa Clara Computer & High Tech L. J.* 145

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

SYMPOSIUM DISCUSSION GROUP REPORT

PRIVACY AND IVHS: A DIVERSITY OF VIEWPOINTS

Margaret M. Russell†

A. CONCERNS

Group members accorded a significant amount of attention to defining the privacy issues potentially raised by Intelligent Vehicle-Highway Systems (IVHS), and expressed widely divergent views on the following initial questions as posed by the facilitator: Are the problems identified by the symposium papers truly "privacy" problems? Is "privacy" (in either a legal or lay sense) an accurate term to describe the complex constellation of concerns raised by IVHS technology?

At the end of the group's deliberations, the facilitator conducted a straw poll on the following three propositions, as formulated by one of the members of the group:

1. IVHS, as presently envisioned, does not present any serious or realistic privacy concerns;
2. IVHS, as presently envisioned, presents serious privacy concerns, but these concerns can be addressed adequately through the adoption of stringent safeguards which will evolve reasonably over time;
3. IVHS, as presently envisioned, presents such serious privacy concerns that there is substantial justification to halt current efforts until these concerns can be addressed.

In true reflection of both the diversity of viewpoints in our group and the ambivalence of individual members over the course of a two-day symposium, the final vote tally was: one vote for proposition 1; six + one half + one half votes for proposition 2; and two + one-half + one-half votes for proposition 3!

To summarize some points of the arguments, at least one member of the group perceived no privacy problems at all with IVHS as currently envisioned, because such systems simply involve the gathering

† Assistant Professor of Law, Santa Clara University.

of data about public comings and goings. According to his argument, no one has a right *not* to be watched when engaged in public activities in a public place (e.g., driving on an interstate highway),¹ and therefore no privacy rights are being abridged by IVHS recordation of these activities.

Other group members, those voting for proposition 3, strongly believed that privacy concerns are inherent in the development of IVHS. They were persuaded by Professor Reiman's use of the "Panopticon" metaphor to argue that otherwise innocuous random data-gathering assumes an Orwellian and sinister aspect when it results in the ready availability of an informational "composite" about a particular individual or individuals.

Still other members, supportive of proposition 2, took a "middle ground" in seeking to define the overall problem; they saw nothing intrinsically invasive in IVHS, but rather identified the potential for abuse in *how* IVHS is used, by whom, and with what degree of controls.

Many group members found several of the presenters' references to literary metaphor and imagery (e.g., Professor Halpern's "traffic in souls," Professor Weisberg's "legacy of Dr. Faustus") useful as part of a conceptual framework for identifying some of the intangible effects of IVHS on autonomy, dignity, and identity. While some members argued that Orwellian fears are exaggerated, ill-founded, and vastly premature, others responded that our collective societal commitment to individual freedom requires us to consider the "worst case scenario" in assessing the potential problems of IVHS.

Finally, group members articulated the following additional concerns about IVHS: loss of personal safety; loss of personal autonomy; harmful error in data-gathering; the selection of IVHS decisionmakers (should they consist of both private and public sector policy makers? How should they go about formulating standards and norms?).

B. SUGGESTIONS

Regardless of members' individual views of the scope of problems arguably posed by IVHS, all agreed that adequate controls must exist to regulate the compilation, retention and dissemination of information. The group was sympathetic to Sheri Alpert's position that some of the controls and protections envisioned below might be explicitly incorporated into federal laws, analogous to what has been

1. The group used as an initial and quite simple example of such technology the installation of electronic beepers or tags on vehicles, enabling the vehicles' (and occupants') whereabouts on public highways to be tracked.

done in the Privacy Act of 1974 and the 1988 Electronic Communications Privacy Act.

1. Whenever possible, personal identifiers should be eliminated. For example, in tracking vehicular movement, vehicle IDs or computer-generated secret codes are preferable to personal IDs. There should be stringent controls on the creation of such IDs and codes.

2. Most group members thought it essential that questions regarding the boundaries of informational access be decided explicitly and carefully *before* the information is gathered. The group concluded that the incidental and inadvertent gathering of surplus data should be avoided; one member expressed the strong view that all such data (i.e., information non-essential to IVHS purposes) should be immediately destroyed to ensure against dissemination and misuse.

3. Several members opined that the risks of invasion of privacy posed by IVHS are so great that this technology should be restricted to the compilation and retention of aggregated information rather than individualized information.

4. Many members agreed that IVHS must incorporate notions of appropriate notice and individualized consent before information is gathered, even in an anonymous, aggregate fashion. Several members stressed that "consent" must be defined to take into account disparities in bargaining power between the data-gatherer and the individual.

5. Group members were divided on the topic of the dissemination of IVHS-gathered information for non-IVHS uses. Some thought that such data should never be made available for non-IVHS purposes. Others stated that it was unrealistic to keep such information, once gathered, from law enforcement officials, but that officers should meet a warrant requirement before obtaining it. Still others in the group held the view that perhaps private entities should be able to purchase IVHS-gathered information for their own uses, subject to the requirements of (1) informed consent of the individual; and (2) an adequate "audit trail" of requests for data. One member stated that especially strict controls should be instituted to prevent insurance companies from securing IVHS-gathered information.

