Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 11 | Issue 1 Article 12

January 1995

Working Towards Fair Information Practices: A Report

Kerry L. Macintosh

SYMPOSIUM DISCUSSION GROUP REPORT

WORKING TOWARDS FAIR INFORMATION PRACTICES: A REPORT

Kerry L. Macintosh†

Over the course of two days, the participants in our discussion group grappled with the privacy implications of Intelligent Vehicle Highway Systems (IVHS). Our views were diverse and often strongly held; many discussions were highly emotional, and unanimity was rarely achieved. Accordingly, this report does not attempt to capture the full richness and detail of our discussions, but seeks merely to state some tentative conclusions we reached about the relationship of IVHS to privacy, and the need for fair information practices that could protect privacy without unduly restricting the efficacy of IVHS technology.

A. CONCERNS

Following extensive discussions regarding privacy and its relationship to IVHS, we concluded that much IVHS data would not concern identifiable individuals, and therefore would not prejudice privacy interests. However, IVHS does have the potential to collect at least some personally-referable data, thereby infringing upon privacy interests. Moreover, several of us found Professor Reiman's analogy of the Panopticon compelling. The potential for integration of IVHS data with the vast amount of data already being collected by governmental agencies and private entities heightened our privacy concerns.

Some participants disagreed, strongly urging that the collection and retention of even individualized information about acts committed *in public* would not infringe upon recognized privacy rights. These same participants tended to view concerns about the development of a menacing Panopticon as speculative and overblown.

† Associate Professor of Law, Santa Clara University.

B. SUGGESTIONS

Our sessions quickly revealed that there were no simple ways to assuage the deeply felt concerns that many participants expressed regarding the impact of IVHS upon privacy.[1] Indeed, many of our discussions involved critique of our own proposed solutions. Nevertheless, most of us agreed that privacy protections should be put into place *now*—before IVHS is fully implemented, and before governmental and private entities become accustomed to having free access to IVHS data. Accordingly, we concluded that the best solution to privacy concerns in the IVHS arena was the implementation of the following fair information practices.

1. *Privacy Impact Statement*: Before IVHS technology is implemented, a "Privacy Impact Statement," similar to the Environmental Impact Statements already required under federal law, should be prepared.

2. *Data creation and retention*: We generally agreed that those who implement IVHS should be careful about the ways in which data is created. Use of "smart cards" and similarly anonymous devices could help us avoid the unnecessary creation of personally intrusive data.

To the extent that IVHS technologies require the creation of at least some personally-referable data, many of us concluded that such data should be destroyed once traffic management objectives have been achieved. However, at least one participant noted that persons involved in commercial vehicle operations (CVO) may need such data in order to comply with otherwise burdensome regulatory duties, such as collecting taxes from truckers on behalf of various governments.

3. *Restrict access to data*: Many participants concluded that privacy could and should be protected by restricting access to IVHS data to those with legitimate traffic management purposes.

Generally, we recognized that law enforcement agencies and personnel would often have a legitimate need for access to IVHS data; however, vigorous debate could not resolve our differences regarding the conditions of such access. Some would allow law enforcement unrestricted access to the data, whereas others insisted that a court order or subpoena should be obtained first.

---

1. One participant questioned the assumption that the implementation of IVHS was necessary; in her view, we should first decide whether the goal of improved traffic management was important enough to outweigh the risks posed to privacy interests.

However, the majority of participants felt that the implementation of IVHS was already a "done deal" and that our best strategy was to make sure that appropriate protections were adopted now, before the technology progressed any further.

Beyond these broad propositions, we could not reach agreement regarding access to IVHS data. One participant argued that private companies needed access to commercial vehicle operations data for legitimate business reasons unrelated to traffic management purposes. Another member of our group unleashed a firestorm of protest by suggesting that, given public resistance to taxes, governments might seek to fund IVHS by selling personally-referable data to private entities for use in marketing. The vehemence of this particular discussion suggests that the need for funding, and the source of funding, could become a major stumbling block to the implementation of IVHS. Perhaps, as yet another person suggested, the solution lies in designing IVHS services that are so desirable —not to mention respectful of privacy—that individuals and companies are willing to pay for them.

4. *Ensuring accuracy of data*: Recognizing the potential for harm to individuals who are falsely identified through IVHS data, we agreed every effort should be made to ensure that only accurate data be collected, retained, and released.

5. *Disclosure and informed consent*: We also reasoned that system users should be fully informed about IVHS capabilities and policies regarding the collection, retention, and release of data. Such disclosure could protect privacy by giving individuals the opportunity to give their informed consent to IVHS participation.

Some participants urged that IVHS should be designed to permit maximum freedom of individual choice, thereby providing a systemic solution to privacy concerns that ultimately would be more effective than legal regulation and sanctions. Freedom of choice would benefit not only those who value privacy, but also those who value the right to choose IVHS. One participant emphasized that the right to choose IVHS was particularly important in the commercial vehicle operations context, where IVHS technology has become an essential means of allowing companies to compete on an international basis.

However, several other participants expressed a deep skepticism about the efficacy of choice or consent as a means of privacy protection. These participants noted that most IVHS technologies could quickly become universal in their application, leaving the individual no choice but to participate and "consent." Indeed, one participant expressed concern that nonparticipation in IVHS would itself become information, and be used to infer guilt rather than legitimate exercise of privacy rights.

Even so, most of us agreed that providing the public with information regarding IVHS objectives and capabilities was worthwhile. Disclosure could actually facilitate implementation of IVHS technol-

ogy, both by allaying unfounded fears about privacy invasion, and by enabling private industries to design products that provide the mix of privacy and traffic management services that consumers actually prefer. In extreme cases, a well-informed public could have the power to reject IVHS applications viewed as unduly oppressive.

6. *Sanctions*: Finally, we recognized that fair information practices could serve to protect privacy only so long as they were consistently observed. Accordingly, criminal sanctions and civil liability should be imposed for unsanctioned use of IVHS data. Such sanctions and liability could help create a culture of compliance with fair information practices.

These solutions that we have proposed—at the end of only two days of discussion—are broadly stated, and undoubtedly underinclusive. While we have not yet, and may never, achieve perfect solutions, most members of our group would probably agree that our discussions were a valuable means of exploring our differing views towards privacy, and the impact that IVHS is likely to have upon privacy.