1995

Is ITS It? Some Conclusions About the Panopticon

George J. Alexander
Santa Clara University School of Law, gjalexander@scu.edu

SYMPOSIUM DISCUSSION GROUP REPORT

IS ITS IT? SOME CONCLUSIONS ABOUT THE PANOPTICON

George J. Alexander†

As a "facilitator" of one of the small groups, I face a number of problems in reporting our discussions. The main problem lies in the expertise and conviction of the group. It included the Co-Director of the Conference and the author of the paper decrying the panopticon while suggesting that it is potentially descriptive of IVHS (now, it appears, reborn as ITS[1]), to mention only the two authors whose expertise in the field was most intimidating to the author. Other members, many with equally extensive backgrounds, should have made it risky for the remainder, such as the "facilitator", who are relative novices, to venture opinions. The final problem was that, despite that fact, the group was quite vocal and often of several minds.

What follows is a report of major themes as I understood them, with apologies for possible misunderstandings and misdescriptions of opinions proffered as well as for the unwitting subordination of some of the participants' opinions to my own point of view.

A. Concerns

The group began on a cantankerous note by questioning whether there was sufficient information on which to base recommendations. It noted that none of us had any experience with the implications of perfect recall of even our own lives. We could only briefly grasp the changes that would accompany our own ability to know such things in complete privacy. We briefly noted how important it is to the life experience we bring to this problem usually to be able to say, honestly, that we cannot speak to one or another issue because we do not have the requisite recall. If we had perfect recall, even assuming that no one could access it but we ourselves, would we all be obliged to help resolve issues in public and private litigation concerning events

† Professor of Law, Santa Clara University.

[1] Intelligent Transportation Systems. The name change connotes an expansion of the regulated field and, consequently, appears to magnify such privacy problems as exist.

which we observed as disinterested bystanders? Would the police expect everyone at a crime scene to assist in the crime's solution? What would happen to polite excuses for missing events we do not want to attend? What, indeed, would happen to the very useful institution of the "white lie"?[2]

If we project the concern about our relative innocence respecting perfect memory to a system in which the data would be held by others, can we even begin to speculate on its potential? If, further, one considers the potential for amalgamation of all data available in separate files, the possibilities become staggering.

The concern about our lack of experience led to some questions about the extent to which ITS really would collect information not already available (and, therefore, of sufficient value to attract private capital). In part, some of us thought, the information may already exist, redundantly, in the private banking, credit card, and telephone records, not to mention far more revealing public records such as income tax forms and social security data. Perhaps, some speculated, what is presently missing is not additional data but adequate data processing at affordable rates. This view is somewhat supported by an article appearing in the *Wall Street Journal* shortly after the conference[3] which suggested that a breakthrough in parallel processing was just now making economic use of available data possible. One wonders how much travel related data would add.

In any event, our skepticism about the commercial utility of personal data did not harden us to ignore the possibility that ITS data might, in fact, breach more privacy boundaries. We briefly discussed the enormity of privacy problems arising from data already available. The recent revelation that some employees of the Internal Revenue Service had been browsing through tax returns of people they knew demonstrated dramatically how all the data that is made available to government makes possible invasions of private information from casual perusal. If the government were to make a concerted effort to amalgamate all of the information about individuals it presently has in separate files, it would create dossiers of unthinkable range.

[2] Dr. Marvin Bressler, retired Chair of Sociology at Princeton University, is presently writing a treatise on lying. My discussions with him have persuaded me that a serious case can be made for lying being an essential optional form of communication in our society. This, of course, does not argue for its indiscriminate use.

[3] *Using Computers to Divine Who Might Buy a Gas Grill*, WALL ST. J., Aug. 25, 1994, at B1, Col. 3.

B. Suggestions

1. In that light, some felt concerned that there was no general set of accepted privacy-based limitations already in place which would simply govern ITS as part of a broader scheme. We all shared the view that collected information should generally not be aggregated with information from other sources.

2. We recognized the potential for claims from many different constituencies for individually identifiable ITS data to meet their own needs and noted that some would be harder to ignore than others. For example, at least one of us thought that such use in the interests of law enforcement should be authorized because of the public priority given to stopping crime. Many of us did not agree either with that specific example or with others. Most of us thought that the information generated by ITS should, to the extent possible, be maintained only in records not identifying individual users.

3. We thought there would be little objection to comprehensive Congressional regulation of such problems. Even for portions of an ITS system which were not federally funded, we thought that the Constitutional authorization of federal power concerning interstate commerce[4] would more than suffice to authorize federal standards for all suppliers and users.

We thought that such regulations should prohibit use of any individually identifiable data for purposes not directly and importantly related to ITS (except for the few who thought law enforcement should also qualify). Consequently we thought that designing the system's structure to operate on depersonalized data in the first place would best accomplish that end. We had in mind the model of public transit electronic cards which are purchased in one place and then provide a passage at another without identifying the user. Of course, we have not paid much attention to how such a system could be designed mechanically but feel fairly certain that engineers would be able to create an inexpensive device.

The system we suggest could handle even quite complex distinctions among cars. For example, if it were important to classify vehicles by their electronic equipment, their roadworthiness, their seating capacity, or anything else, it should be possible to have a two step process. In step one, the driver or owner would qualify the vehicle in whatever manner required. At the end of the qualification process, instead of providing a sticker or certificate, the state would supply a token which entitled the driver of the vehicle to get access to the anon-

[4] U.S. Const. art. 1, § 8.

ymous card-issuing machine. The token could be individuated to any extent desired so long as the ultimate pass-granting machine recorded nothing which would identify the individual driver or vehicle. The pass-issuing machine could issue passes limited to certain uses, speeds, destinations or whatever factors are of importance to the ITS administration so long as the machine was not designed to read any individuating data from the token and so long as the qualification itself did not tend to identify the user.

4. Regulations governing the acquisition of information should allow the release of user-identifiable information as sparingly as possible (not at all if possible). If information that identifies users is collected, regulations should limit its retention to as short a period as possible. Those provided access should be only those with a need to know, and strong regulations should prevent further disclosure. It is precisely because such safeguards have not always been successful in the past that we favored placing privacy concerns directly in the design on information acquisition.

We noted, with great pleasure, that the conference and its discussions, for once, preceded implementation. Often law is applied to technological advances only much later in the process. We thought that the early airing of issues would make it possible to design a system that would raise fewer problems than one built with only efficiency concerns as a guide. We particularly thought that the government should be commended for providing this early opportunity for these discussions.