Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 11 | Issue 1 Article 9

January 1995

Computerized Highways and the Search for Privacy in the Case Law

Ronald D. Rotunda

COMMENT

COMPUTERIZED HIGHWAYS AND THE SEARCH FOR PRIVACY IN THE CASE LAW

Ronald D. Rotunda†

The new technology governing intelligent highways is like a knife that cuts both ways. It should give us, for example, greater fuel efficiency, and speedier and safer travel. However, it can also give us less privacy in the use of the highways.

In one sense, we are told not to worry. After all, in the old days, when most people lived in small towns, everyone knew everyone else, and there were no secrets. Town gossips quickly told and retold everything, but "gossip," unlike "privacy," is a word that has pejorative connotations.[1] People generally do not like to have others gossip about them, and, as they moved to the cities, they valued the privacy that larger cities afforded them.

The new computerized technology, with its ability to collect, store, retain, catalog, and retrieve massive amounts of data with lightening speed and accuracy, has the ability to challenge this privacy.

We are also told that what happens on the public streets and sidewalks is not private, and so intelligent highways do not really implicate privacy at all. In one sense, this is true. Anyone can see your car and its unique license plate when you travel on the city streets. The Supreme Court elaborated this fact in *United States v. Knotts*,[2] when it held that there was no Fourth Amendment violation, no unlawful search and seizure, if the police monitor the signal of a beeper placed in a container of chloroform that was transported by car from Minnesota to a cabin in Wisconsin.

The authorities in *Knotts* secured no search warrant to install their beeper. The chemical company officers had consented to the

† The Albert E. Jenner, Jr., Professor of Law, University of Illinois College of Law. In writing this article, I am indebted to my colleague, John Nowak, for our many conversations regarding privacy, its importance, and its protection.

1. *See generally*, RONALD D. ROTUNDA, THE POLITICS OF LANGUAGE (U. Iowa Press, 1986), (explaining how words both mold and reflect the way we think).

2. 460 U.S. 276 (1983).

installation of a beeper inside the five gallon drum of chemicals, but they sold it to the purchasers of the drum, who were ignorant about the beeper. This surreptitious electronic surveillance enabled the police to discover a fully operable, clandestine drug laboratory in the Wisconsin cabin.

Justice Rehnquist, for the Court, rejected the Fourth Amendment claims and held that the monitoring did not violate any legitimate expectation of privacy but only allowed the police to obtain information that the authorities could have obtained through visual surveillance. Justice Rehnquist argued:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When Petschen [one of the defendants] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[3]

Rehnquist went on to explain that while Knotts, another defendant and the owner of the Wisconsin cabin, had a reasonable expectation of privacy "insofar as the cabin was concerned," there was "no such expectation of privacy extended to the visual observation of Petschen's automobile arriving on his premises after leaving a public highway, nor to movement of objects such as the drum of chloroform outside the cabin in the open fields."[4]

One wonders if a layperson would be entirely persuaded by the reasoning in this and similar cases.[5] Granted, the authorities could have stationed a police officer every fifteen feet on the highway, if they knew on which highways the driver would be traveling. However, that tactic is a tad conspicuous, and the people in the car, even if

---

3. 460 U.S. at 281-82. *See also, e.g.*, Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion) "A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view."

4. 460 U.S. at 282, *citing*, Hester v. United States, 265 U.S. 57 (1924). *See also*, Oliver v. United States, 466 U.S. 170 (1984)(holding that the Fourth Amendment does not prevent the government from inspecting "open fields" of a private land owner even though the person had taken steps to prohibit trespassers from entering the land in question.)

5. *E.g.*, Smith v. Maryland, 442 U.S. 735 (1979)(holding that when the telephone company installed, at the request of the police, a pen register device which records the numbers dialed from a telephone, that did not constitute a "search" under the Fourth Amendment because there was no "legitimate expectation of privacy" in the phone numbers that one dials) *and* Florida v. Riley, 488 U.S. 445 (1989)(holding that no search warrant was required when a police officer, in helicopter circling about 400 feet above a partially covered green house in the back of a private home, viewed the interior of the greenhouse and saw marijuana plants).

they were not expecting to be tailed, would have a sense that they were being followed. *Knotts* does not require the police to inform a suspect that he or she is being followed.

Moreover, there is the question of expense, which placed a check on the police in the era before the emergence of modern technology and cheap computing power. Assume that the police are following someone driving on the city streets without the use of a beeper. Even if the suspect would not distinguish the army of undercover agents from all the other people on the streets, the constabulary simply could not afford this army as part of any routine surveillance. The beeper makes doable and economically feasible what would, in earlier years, be a profligate, extravagant fantasy.

Instead of the army of agents, the police could use an undercover vehicle to follow the mysterious drum and the car transporting it. That action would be both more economical and less indiscrete. But if the police did that, the defendants, who could not elude the hidden beeper, could elude the visual surveillance. In fact, that is what happened in *Knotts*. In addition to the beeper, the authorities visually followed the car, but lost it. In fact, the authorities even lost the beeper signal, but eventually found it again with the help of additional, modern technology, a monitoring device in a helicopter.

In short, technology allows the police to engage in surveillance that would otherwise be less furtive and crafty, more difficult, expensive (often prohibitively so), and time consuming. The Supreme Court's analysis in *Knotts* does not take into account these concerns.

In a society without modern technology and computerized retrieval of data, a sleuth with sufficient time and money could accumulate a lot of data about anyone, merely by watching what one does on the public streets, noting where one shops and what he or she buys, watching which magazines are deposited in one's mail box, examining one's abandoned garbage, collecting publicly available court records of birth certificates, divorce decrees, marriage licenses, and so forth.[6] Yet Warren and Brandeis, in their seminal article on privacy published over a century ago, recognized that one does not lose all interest in privacy just because information may, somewhere, be part of some record that is publicly available, and that someone, with a great amount of diligence, may be able to find that record.[7] Or, as Chief Justice Rehnquist noted more recently, that an "event is not wholly

6. *Cf.* Kenneth L. Karst, *"The Files:" Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342, 344 (1966).

7. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890-1891).

'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[8]

Knotts illustrates that the Court has been generally unsympathetic to using the Fourth Amendment to protect privacy claimed to be invaded by the use of the new technology affecting highways and the outdoors. However, it is incorrect to conclude that the Court will be unwilling to protect such privacy interests if the claim is based on other constitutional rights. The jury is still out on that question, but there are suggestions in other cases, not relying on the Fourth Amendment, that may indicate a judicial concern for the privacy implications of the new technology. From these other cases, the Court might fashion tools to expand privacy protection.

I do not mean to suggest that we should only look to the Supreme Court to balance legitimate expectations of privacy with the reasonable needs of law enforcement. As citizens we should not abdicate our own responsibilities. Legislators and regulators, especially when drafting statutes and regulations, should also be sensitive to the needs of privacy in light of increasingly sophisticated technology.[9]

Some people think of the Constitution as a magical piñata that, when hit at the right angle, will give us the answers to all of our social problems. Yet, the fact that something is constitutional does not mean that it wise and just. Because the government may constitutionally be able to place a beeper on a vehicle without obtaining a warrant does not mean that there should never be any legislative or regulatory limits to the collection and retention of data about vehicles on the public highways.[10]

---

8. Hon. William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, NELSON TIMOTHY STEPHENS LECTURES, UNIVERSITY OF KANSAS LAW SCHOOL, 13 (Sept. 26-27, 1974), *quoted in*, United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 770-71 (1989).

9. *Cf.*, Illinois v. Abbott & Associates, Inc., 460 U.S. 557 (1983). A federal law authorized the Attorney General to make federal grand jury antitrust materials available to a state attorney general. The Court held that this statute did not dispense with the normal requirements of a showing of a particularized need by the state for the grand jury material. The Court, thus, limited the Government official's right to disclose information about individuals by its interpretation of the applicable statutes and court rules. *See also*, Detroit Edison Co. v. NLRB, 440 U.S. 301 (1979)(holding that the NLRB cannot compel a company to disclose to a union the results of psychological tests on individual employees unless those employees consented. The Court interpreted the labor laws and concluded that the employee's right to confidentiality outweighed the union's assertion of a need for the data).

10. *See generally*, H.R. Rep. No. 1416, 93d Cong., 2d Sess., 3 et seq., *reprinted in*, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, SOURCE BOOK ON PRIVACY, at 294, 399 (1974), which lists various state laws requiring that computerized, cumulative, indexed criminal historical information be kept confidential.

In short, although a future Court may not use the Fourth Amendment to create new privacy rights in this area, and although legislators, regulators, and the general public should not abdicate their responsibility to be sensitive to, and watchful of, privacy concerns, there may be other constitutional clauses that may supply added protection. Let us look at some of the precedent outside of the Fourth Amendment area[11] to see what tools that caselaw offers future courts to limit government computerized collection and use of data about private individuals.

Whalen v. Roe[12] is one important case to consider. The Court unanimously upheld a New York state law requiring physicians and pharmacists to forward copies of prescriptions for medicines containing narcotics to state authorities. In reaching this conclusion, the Court's reasoning was interesting, because it applied a methodology that did not dismiss the constitutional argument as frivolous; in addition, it suggested some important factors to consider in evaluating the privacy claim. *Whalen* was not a Fourth Amendment case. Rather, the Court considered the liberty, due process interest of the patients and doctors objecting to the reporting, retention, and possible abuse of the information collected.

Justice Stevens, for the majority, found that the state law related to the legitimate and "vital" function of controlling illegal drug distribution.[13] Furthermore, the law was reasonable in its limitations on the use and distribution of the collected data. The mere possibility that the data would be improperly used did not void the law on its face. The Court thus concluded that the state law, on its face, did not violate any privacy expectation that the government not make an individual's private affairs public.[14]

The Court also turned to another aspect of privacy. The appellees had argued that even if unwarranted public disclosures do not actually occur, "the knowledge that the information is readily available in a computerized file creates a genuine concern that causes some persons to decline needed medication."[15] The Court rejected this argument as well because, although there was evidence that some people may have been discouraged from using medication by the existence of the computerized data files, "it also is clear, however, that about 100,000 prescriptions for such drugs were being filled each month

11. On the fourth amendment, *see generally*, WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (2d ed. 1987)(with annual pocket parts).

12. 429 U.S. 589 (1977).

13. 429 U.S. at 598.

14. 429 U.S. at 600.

15. 429 U.S. at 602-03.

prior to the entry of the District Court's injunction. Clearly, therefore, the statute did not deprive the public of access to the drugs."[16] Thus, the Court found that there was no violation of any liberty interest under the Fourteenth Amendment.

Significantly, in considering the privacy implications of the computerized file of information, the Court added a cautionary note: "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." Justice Stevens, for the Court, admitted that the government must collect and preserve a lot of information related to the collection of taxes, the distribution of welfare benefits, the supervision of public health, and so forth. Much of this information "is personal in character and potentially embarrassing or harmful if disclosed." Thus, the

> right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty *arguably has its roots in the Constitution*, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data — whether intentional or unintentional — or by a system that did not contain comparable security provisions. We simply hold that *this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.*[17]

Justice Stevens thus left open the opportunity for the Court to find a constitutional privacy interest in a case where the record showed that the accumulation of vast amounts of personal information in computerized data banks was not accompanied by a statutory and regulatory scheme that evidenced "a proper concern with, and protection, of, an individual's interest in privacy." This duty, said the Court, "arguably has its roots in the Constitution."

Justice Stewart, concurring, was the only Justice who disassociated himself from the implications of the majority opinion.[18] In contrast, Justice Brennan's concurring opinion welcomed them. Brennan recognized that the central storage and easy accessibility of computerized data "vastly increase the potential for abuse of that information,"

16. 429 U.S. at 603.

17. 429 U.S. at 605-06 (emphasis added).

18. 429 U.S. at 608-09 (Stewart, J., concurring).

and foresaw that future developments might demonstrate the necessity of some curb on such technology. In this case, because New York's "carefully designed" statute limited access and prevented abuse, Brennan agreed with the opinion of the Court that the law, on its face, did not deprive anyone of any "constitutionally protected privacy interests." But if the statute, on its face or as applied, did create such a deprivation, it "would only be consistent with the Constitution if it were necessary to promote a compelling state interest."[19]

United States Department of Justice v. Reporters Committee for Freedom of the Press,[20] lends support for the concerns that the majority and Justice Brennan expressed in *Whalen*. In *Reporters Committee* the Court held that events summarized in FBI's rap sheets regarding individuals was exempt from disclosure by the Freedom of Information Act.[21] In *Reporters Committee* it was argued that the privacy interests of the individuals on whom information was collected and retained in these rap sheets "approaches zero" because all the information had previously been disclosed to the public.[22] The Court rejected that "cramped notion of personal privacy."[23]

Without a dissent, the majority noted that the common law "recognized a privacy interest in matters made part of the public record."[24] The Court went on to explain that there is a difference between "scattered disclosure of the bits of information contained in a rap sheet and [the] revelation of the rap sheet as a whole."[25] Government resources create and maintain the files and the indexes, making easily available information that otherwise would be difficult and expensive to maintain and retrieve. Significantly, the Court added:

> Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.[26]

---

19. 429 U.S. at 607 (Brennan, J., concurring)(*citing* Roe v. Wade, 410 U.S. 113 (1973)) and Eisenstadt v. Baird, 405 U.S. 438, 464 (1972)(White, J., concurring). *Roe* dealt with a right to abortion and *Eisenstadt* dealt with access to birth control pills and devices by unmarried people.

20. 489 U.S. 749 (1989).

21. 5 U.S.C.A. § 552(West 1977).

22. 489 U.S. at 763.

23. *Id.*

24. 489 U.S. at 763 n.15. The Court acknowledged that the privacy interest was diminished and a private person who obtained the information might be privileged to publish it, citing Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 494-95 (1975).

25. 489 U.S. at 764.

26. 489 U.S. at 764.

The Court, after referring several times to the impact of computerized data banks on individual privacy, concluded that disclosure of the FBI rap sheets to third parties would constitute an unwarranted invasion of personal privacy and was thus exempt from disclosure under the Freedom of Information Act.[27]

In the First Amendment arena, the Court has also found some protection for a right of privacy related to accumulation and retrieval of information. In these cases the focus, thus far, is more on compelled disclosure of private facts rather than computerized collection and retention of personal data. However, a basic principle that may lie behind these cases is that privacy concerns should impose a requirement that government behave reasonably in collecting and protecting the confidentiality of such data.

For example, the Court has limited, under the First Amendment, the applicability of a campaign disclosure law requiring political parties to disclose the names of their members and contributors. Such a law is not invalid on its face, but it is unconstitutional as applied to minor parties who demonstrate that they are subject to private or government hostility and that thus disclosure will impair the free speech rights of the minor political parties.[28]

The Court, also relying on the First Amendment, has invalidated laws banning unsigned handbills,[29] or compelled disclosure of membership lists of organizations[30] unless the laws were narrowly tailored to promote a compelling or substantial government interest.

In *Doe v. McMillan*,[31] the Court narrowly interpreted the Speech and Debate Clause[32] to protect privacy concerns. In that case, parents of the school children in the District of Columbia sued members of the House Committee on the District of Columbia. The plaintiffs also sued employees of the Government Printing Office. The plaintiffs sought damages, and declaratory and injunctive relief for alleged inva-

27. *Cf.* Thornburgh v. American College of Obstetricians and Gynecologists, 476 U.S. 747, 766-68 (1986). In the course of invalidating various state restrictions on abortions, the Court turned to the state regulation requiring doctors to report the basis for their decision that a fetus was not viable. Although the regulations did not require that the doctors' reports identify the name of the women seeking an abortion, other information made it possible to identify these women, and these reports were open to the public. The majority thus invalidated the requirement of collecting this information because it violated the woman's right to privacy, by allowing the disclosure of private facts.

28. Brown v. Socialist Workers '74 Campaign Committee, 459 U.S. 87 (1982).

29. Talley v. California, 362 U.S. 60 (1960).

30. *Compare* N.A.A.C.P. v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958) *with* New York *ex. rel.* Bryant v. Zimmerman, 278 U.S. 63 (1928) *and* Gibson v. Florida Legislative Investigation Committee, 372 U.S. 539 (1963).

31. 412 U.S. 306 (1973).

32. U.S. CONST., art. I, § 6.

sion of privacy resulting from the public dissemination of a committee report on the District of Columbia school system. This report identified students by name, and spoke in a derogatory manner about them, calling them, for example, "class cutters."

While the Court ruled that the Speech or Debate Clause immunized the members of Congress and their alter egos,[33] the Court was less protective when it turned to the public printer and the superintendent of documents, who had printed excess copies of the report for use other than internally by Congress. The Court held that the plaintiffs had a cause of action against these other defendants. These defendants were not immune under the Speech or Debate Clause because, even though the act of distributing excess copies of the reports informed the public, informing the public was not "an integral part of the deliberative and communicative processes by which Members participate in committee and House proceedings."[34] As the Court said in an earlier case, "no doubt there is no congressional power to expose for the sake of exposure."[35]

Cases such as *Whalen v. Roe*, *United States Department of Justice v. Reporters Committee for Freedom of the Press*, and *Doe v. McMillan* do not overturn the results of *United States v. Knotts*. However, the cases do illustrate that there may be, outside of the Fourth Amendment, constitutional protections for privacy in the context of the collection, retention, retrieval, and use of computerized data involving the use of the public highways. Even if later opinions do not dramatically build and expand upon these cases, they do indicate that the Court, as well as the rest of us, should be sensitive to the novel problems created by the ability of modern technological devices to collect and store vast amounts of data about large numbers of individuals, and the ability of cheap computer power to manipulate, organize, retain, and retrieve this data in ways that affect the privacy of us all.

33. *I.e.*, the committee staff and the consultant to the committee and the investigator introducing material at the committee hearings.

34. 412 U.S. at 314.

35. Watkins v. United States, 354 U.S. 178, 200(1957).