



Volume 22 | Issue 6


Article 5

1976

Computers and the Right to Be Let Alone - A Civil Libertarian View

Burton Caine

Follow this and additional works at: <https://digitalcommons.law.villanova.edu/vlr>

 Part of the [Criminal Law Commons](#), and the [Criminal Procedure Commons](#)

Recommended Citation

Burton Caine, *Computers and the Right to Be Let Alone - A Civil Libertarian View*, 22 Vill. L. Rev. 1181 (1976).

Available at: <https://digitalcommons.law.villanova.edu/vlr/vol22/iss6/5>

This Symposia is brought to you for free and open access by Villanova University Charles Widger School of Law Digital Repository. It has been accepted for inclusion in Villanova Law Review by an authorized editor of Villanova University Charles Widger School of Law Digital Repository.

COMPUTERS AND THE RIGHT TO BE LET ALONE —
A CIVIL LIBERTARIAN VIEW

BURTON CAINE†

Almost fifty years ago, Justice Louis Brandeis in his famous dissent in *Olmstead v. United States*,¹ wrote:

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men.²

In a five to four decision, the Supreme Court in *Olmstead* held that wiretapping violated neither the fourth amendment proscription against unreasonable search and seizure³ nor the fifth amendment protection against self-incrimination.⁴ Justice Brandeis disagreed on both points and condemned "every unjustifiable intrusion by the Government upon the privacy of the individual"⁵ as a violation of "the right to be let alone."

For a generation, Justice Brandeis had been reflecting upon this "right most valued by civilized men." In 1890, Justice Brandeis, together with Samuel D. Warren, wrote an article entitled *The Right to Privacy*,⁶ which identified and gave name to the right for the first time in American jurisprudence. It was not until 1965 that the Supreme Court of the United States confirmed the existence of a right of privacy. In *Griswold v. Connecticut*,⁷ the Court invalidated a law against contraceptives as an unconstitutional interference with the privacy of the marital relationship. The justices found that various provisions of the Bill of Rights formed a "penumbra"

† Professor of Law, Temple University; Lecturer in Law, University of Pennsylvania; Chairman, Subcommittee on Privacy of the American Civil Liberties Union; Member, Board of Directors, American Civil Liberties Union; Partner, Wolf, Block, Schorr & Solis-Cohen. A.B., University of Pennsylvania, 1949; J.D., Harvard University, 1952.

1. 277 U.S. 438 (1928).

2. *Id.* at 478 (Brandeis, J., dissenting).

3. *Id.* at 466.

4. *Id.* at 462.

5. *Id.* at 478.

6. 4 HARV. L. REV. 193 (1890). See Pollak, *The Right to Be Let Alone*, 38 PA. B.Q. 399 (1967).

7. 381 U.S. 479 (1965).

guaranteeing a right of privacy to the individual against unwarranted intrusion by the government. Despite the absence of an explicit reference, a right of privacy was implied. The Court cited the ninth amendment which provides that rights enumerated in the Constitution shall not be construed to deny other rights retained by the people. The right of privacy, the Court said, derived from "several fundamental constitutional guarantees" and in the case of the marital relationship, the "right of privacy [is] older than the Bill of Rights."⁸

The American Civil Liberties Union (ACLU), on whose behalf I speak, vigorously contends that government compilation of dossiers and files on its citizens poses grave dangers to the right of privacy, or the right to be let alone. ACLU concedes that court decisions have failed to confirm the full implications of the right of privacy suggested in *Griswold v. Connecticut* or the Brandeis dissent in *Olmstead v. United States*. Unfortunately, the Supreme Court of the United States has held in *Laird v. Tatum*,⁹ that the mere existence of government intelligence gathering and maintenance of files is not unconstitutional. As the law now stands, some abuse of the files must be shown, for example, where city officials disclose information from surveillance files on national television.¹⁰

Nor is it clear upon which provision of the Bill of Rights a resting place will be found for the individual's right to be free from dossier building by the Government. ACLU urges those who cherish liberty to oppose such systems as violations of the right of privacy — the right to be let alone.

Free citizens sense danger in files maintained on them by the government. There are chilling implications in the phrase "the government has a file on you," and the terminology is illuminating. It was enough for Aryeh Neier, Executive Director of the American Civil Liberties Union, to entitle his book *Dossier*, with a subtitle "The Secret Files They Keep On You."¹¹ The growing capacity of computers and their ability to store, coordinate, and transmit information have increased the dangers to the privacy of ordinary citizens to the point of alarm.

Congress may be more sensitive than the Supreme Court to the dangers to privacy lurking in computerized information systems. In

8. *Id.* at 485-86.

9. 408 U.S. 1 (1972). See also *California Bankers Ass'n v. Shultz*, 416 U.S. 21 (1974).

10. *Philadelphia Yearly Meeting of the Religious Soc'y of Friends v. Tate*, 519 F.2d 1335 (3d Cir. 1975). See also *Socialist Workers Party v. Att'y Gen.*, 419 U.S. 1314 (1974).

11. A. NEIER, *DOSSIER* (1975).

the Privacy Act of 1974,¹² Congress provided for individual safeguards against invasion of personal privacy by the federal government. The congressional findings include the unequivocal statements that

the right to privacy is a personal and fundamental right protected by the Constitution of the United States.

[T]he privacy of an individual is directly affected by the collection, maintenance, use and dissemination of personal information by Federal agencies and . . . [that] . . . the increasing use of computers and sophisticated information technology . . . has greatly magnified the harm to individual privacy.¹³

The Privacy Act also establishes a Privacy Protection Study Commission to examine the handling of the government information and make recommendations. The report is expected in June, 1977. David F. Linowes, Chairman of the Commission has stated: "I seriously believe that at some point in the not-so-distant future, data collections, maintenance and dissemination may no longer be merely a tool of society, but will instead become an end in itself — a force with awesome powers of surveillance and control over the lives of individuals."¹⁴ One reason for the concern is that according to a report entitled *Federal Personal Data Systems* published pursuant to requirements of the Privacy Act of 1974, the federal government today maintains 6,723 different record systems containing a total of 3.9 billion individual files, or eighteen files for every man, woman and child in the United States! With the increasing ability of computers to link one with another, not only in government but with private industry, we are facing a technology run wild.

Last year, for example, the Bell Telephone system furnished to federal agencies billing records of 20,565 customers. Moreover, a study being completed by the Privacy Commission staff shows that the principal government users of commercial data are the Federal Bureau of Investigation and the Internal Revenue Service. Requests are also made by the Central Intelligence Agency, the Securities and Exchange Commission, the Federal Energy Administration and the Drug Enforcement Agency.¹⁵ Billions of personal records are kept by

12. 5 U.S.C. § 552a (Supp. V 1975).

13. Privacy Act of 1974, Pub. L. No. 93-759, § 2(a)(4), (a)(1), (a)(2), 88 Stat. 1897 (1974) (codified at 5 U.S.C. § 552a) (Supp. V 1975).

14. See Stanford, *What's Happening to Your Privacy?* PARADE, Feb. 27, 1977 at 24.

15. According to The New York Times, the Commission is expected to recommend severe restrictions on the government's right to access to records in the private sector without consent of the individual involved. N.Y. Times, May 15, 1977, at 28, col. 1.

commercial institutions such as credit card companies, airlines, banks, retail chains. According to a preliminary staff estimate, three of the largest credit agencies in the United States have a total of more than one hundred million names on file. The Medical Information Bureau, which supplies information to insurance companies, has medical records of approximately 12.5 million people, and one mailing list company boasts that it has over seventy million names.

The government's shabby record on violating individual rights increases the dangers to civil liberties. Spying, harassment, surveillance, wiretapping, burglaries, intimidation, threats, dossier building, misuse of grand juries, have unfortunately become the hallmarks of a government neglecting its sworn duty to uphold the Bill of Rights.

It is important to note and to emphasize that the first ten amendments to the Constitution of the United States were designed to limit the power of government in order to protect the rights of the individual. Admittedly, government might work more smoothly if individual rights could be ignored. But liberty, not efficiency, was the theme of the Bill of Rights and individuals were granted rights as *against* the government.

Even assuming a benevolent government, the possibility of human error alone requires severe limitations on record keeping by the government. Considering the sad history of official misconduct, tight restrictions on record keeping and information systems become mandatory in the highest degree.

The case of *Menard v. Saxbe*¹⁶ is an illustration of what might happen to an ordinary citizen seeking to redeem his right to be let alone. Dale Menard, a student, was sitting in the park and was picked up by the Los Angeles police investigating a complaint that there was a prowler in the vicinity. Menard was completely exonerated, and in all probability the crime for which he was apprehended had never taken place.¹⁷

The police recorded the contact as a detention. The information was immediately sent to the FBI in Washington, which retained it, including fingerprint files and other information growing out of the event. The data were then circulated throughout the United States. It took nine years of litigation simply to have that information expunged from the FBI's criminal records, although the court would

16. 849 F.2d 1017 (D.C. Cir. 1974).

17. *Menard v. Mitchell*, 430 F.2d 492 n.27 (D.C. Cir. 1970). This case was an earlier proceeding in the protracted *Menard* litigation.

not order expungement from the FBI's identification records.¹⁸ Once that legal battle was finally won, Menard was faced with the prospect of having to start litigation against every law enforcement agency in the United States which may have received the misinformation that he was arrested.

Threats to privacy are not limited to criminal records. The New York Times reports that two members of Congress and the Office of Technology Assessment have requested a halt in the development of a one billion dollar computer by the IRS because it poses "a threat to civil liberties, privacy and due process of taxpayers," and could ultimately result in "surveillance, harassment or political manipulation of files."¹⁹ These expressions of concern about the IRS computer are similar to questions raised last year about elaborate computer networks proposed for the FBI, the Federal Reserve System, the Social Security Administration, and the General Services Administration.

To reduce the dangers to the right of privacy, the American Civil Liberties Union recommends the following governing principles for any computerized information system or data bank:

1. No system or data bank should be established unless the need therefor has been proven and the proposed system will meet that need. This requires convincing proof that the present system is not adequate for the task.

2. No information should be recorded unless there is a specific demonstrated need directly related to a lawful and legitimate function of the recorder.

3. No information should be preserved or stored for longer than absolutely necessary to accomplish the purposes for which it has been recorded and expungement should be programmed at the time of the entry of any information.

4. If the information is especially sensitive so as to create extraordinary injury if disclosed, the information should not be recorded.

5. No information should be disseminated to anyone outside of the system. Information should not be given to anyone within the system without an affirmative, demonstrable need to know the particular information and the recipient must be authorized by law to obtain it. Detailed rules on security and confidentiality should be

18. 489 F.2d at 1029. The court found no constitutional right to expungement, the decision being made solely on the ground that the statute empowered the FBI to record only "an arrest" not a detention in its criminal records. *Id.*

19. *Rights Issue Raised On Big Tax Computer*, N.Y. Times, Mar. 16, 1977, at 34, col. 1.

promulgated to enforce this principle and they should leave no doubt regarding exactly who is entitled to what information.

6. All persons with respect to whom information is recorded should be notified of the nature of the information, together with an explicit, intelligible statement that such person has a right to inspect the information at any time for the purpose of correcting inaccuracies, updating the entries, and expunging information improperly recorded or maintained.

7. No information should be disclosed without prior notice to the individual involved of the proposed disclosure and the reasons therefor together with an opportunity to challenge disclosure and to correct and update the information.

8. Information stored should be immune from subpoena, discovery, or other legal process. In addition, employers should be forbidden by law from having access to such information, and from requiring employees to obtain or disclose such information in connection with employment.

9. Any violation of these rules should be made a crime, and should also give rise to civil liability for actual damage caused, with a minimum liquidated damage provision in the event that specific injury cannot be proven. Counsel fees should also be awarded.

10. Finally, a committee of citizens should be appointed to monitor the operation of the information system and promulgate regulations to insure compliance with these rules. The committee should be broad-based and should include government representatives, private citizens, and civil rights groups such as, for example, the American Civil Liberties Union.

In light of these principles, we turn to a consideration of some of the competing interests involved in a computerized criminal justice information system. The first requirement often overlooked is for the proponents of such a system to set forth with precision the exact need for such a system, and specifically how the computerized data bank will meet that need. This includes a demonstration that the present system is not adequate for the task.

In the proposed Philadelphia Justice Information System (PJIS) it is doubtful whether that requirement has ever been met. I have sat in on meetings involving PJIS, I have read articles, including the one which appeared in *Philadelphia Magazine*²⁰ purporting to describe how that system came into being, and I must say that I have not yet seen a satisfactory demonstration of need to satisfy the threshold requirement. Compliance with this requirement should not

20. Guinther, *This Computer is Armed and Dangerous*, PHILADELPHIA MAGAZINE, October 1976, at 89.

be assumed no matter how much time, money, and effort is expended. For example, with respect to the proposed one billion dollar IRS computer, the government's Office of Technology Assessment questioned the need for such a system despite the extensive justification offered by the IRS. In a front page story, *The New York Times* reported that the General Accounting Office "is critical of the Department's computerized crime intelligence system," calling it a costly project of "dubious value."²¹

ACLU is not alone in questioning whether a need has been shown for the proposed Philadelphia Justice Information System. The Honorable Robert W. Williams, Jr., Judge of the Court of Common Pleas of Philadelphia, and Treasurer, Philadelphia Regional Planning Council, under whose aegis PJIS was designed, poses serious and thoughtful questions about the entire program, at least in its present form.²² Judge Williams asserts that after an outlay of thirty million dollars in federal Law Enforcement Assistance Administration (LEAA) state and local funds, there is no clear idea just what PJIS is designed to do and the underlying facts have not been disclosed.

Nor is ACLU aware of any convincing proof that the so-called "Pennsylvania Plan"²³ satisfies the first principle set forth above.

Time and space do not permit review of each of the ten principles and their application to the Philadelphia or Pennsylvania Plans. However, one point relating to the security of the system should be noted here. The Philadelphia Plan contains "Recommended Rules on Standards and Safeguards for the Privacy, Confidentiality and Security of Information in PJIS."²⁴ Peter J. Liacouras, Dean of Temple University School of Law, chaired the Confidentiality Committee of the Philadelphia Regional Planning Council of the Governor's Justice Commission and imbued the Committee with a high sense of purpose in drafting rules to guard the right of privacy. With respect to security Dean Liacouras said:

Whatever information goes into computers will as a practical matter leak out, even if regulations prohibit such dissemination. Consequently, the practical restrictions at the point of what goes into the computer are important rather than who has access to it. Accordingly, the Confidentiality Committee

21. *N.Y. Times*, Mar. 19, 1977, at 1, col. 1.

22. Williams, *Judge Questions Computerization Guidelines, The Retainer*, at 1, col. 1 (Pub. of the Phila. Bar Ass'n, Feb. 4, 1977).

23. Report of Governor's Task Force on Criminal Justice Information Systems. See generally 4 PA. CODE §5.41-.47 (1975).

24. These rules were adopted with revisions by The Philadelphia Planning Council, Governor's Justice Commission, May 10, 1976.

concluded that no information should go into PJIS, the Philadelphia Justice Information System, except that currently available to the public and records now being maintained.²⁵

ACLU applauds this sensitive and realistic approach to securing the right to privacy. The point is simply that the most important element in any security system is restriction on input — not restriction on access.

ACLU has endorsed the PJIS Confidentiality Rules with certain reservations. In contrast, ACLU does not consider the Pennsylvania Plan for Privacy and Security of Criminal History Record Information to be a privacy plan despite its title; rather, it appears to be designed to improve the efficiency of the system.

We have been asked to discuss the competing interests involved in including arrest record information within a computerized criminal justice information system. Arrest records followed by conviction pose no problem because the conviction overshadows the arrest. However, memorializing an arrest not followed by conviction poses a serious civil liberties question. In this situation, ACLU strongly maintains that every record of the arrest be expunged without a trace from any information system, including those to which the notice of arrest may have been transmitted. The vice of an arrest record where no conviction follows is that punishment is imposed where there is no guilt — and even where there is no crime. Not only is the right to privacy invaded, but violations of due process and protection against cruel and unusual punishment are also involved.

In the *Menard* case, Judge Bazelon described some of the harm an individual might suffer from having an arrest record:

Even if no direct economic loss is involved, the injury to an individual's reputation may be substantial. Economic losses themselves may be both direct and serious. Opportunities for schooling, employment, or professional licenses may be restricted or nonexistent as a consequence of the mere fact of an arrest, even if followed by acquittal or complete exoneration of the charges involved.²⁶

Despite their innocence before the law, persons with an arrest record are subjected to severe, continuing, and pervasive punishment simply because they have "a criminal record." The government is

25. Remarks of Peter J. Liacouras in Connection with Proposed Amendments to Recommended Rules for PJIS (March 24, 1976).

26. *Menard v. Mitchell*, 430 F.2d 486, 490 (D.C. Cir. 1970) (footnotes omitted).

the largest employer in the country. Why should a government personnel officer in choosing among several applicants take a chance and ignore a "criminal record" when he has applicants who have never been arrested? Why should he run the risk that the press or other critics will charge that the government hires criminals?

In addition, the police and the criminal justice system take into account an arrest record in determining whether to arrest an individual, whether to bring formal charges against the person already arrested, and for numerous other purposes adverse to the individual.²⁷

The probability of arrest for urban males is quite high. For urban black males the probability of arrest at least once during a lifetime has been estimated to be as high as 90%. For white urban males the figure is 60%, and for all males it is 47%.²⁸ Fewer than 25% of those arrested per year are found guilty of the offense for which they were arrested, and only a little more than 25% are found guilty of any crime at all.²⁹ As the statistics show, the punishment which flows from an arrest record works a disproportionate disadvantage against blacks in the ghettos in cities throughout the United States. Again, quoting Judge Bazelon, "if the person arrested has been exonerated it is difficult to see why he should be subject to continuing punishment by adverse use of his 'criminal' record."³⁰

An arrest without conviction is as much an indication of unlawful activity by the police as by the person arrested; yet, nothing appears on the criminal record of the policeman for having committed an unlawful act. When the policeman applies for credit or for a job, there is no notation of law infraction. Even if it makes a difference whether the police officer has probable cause for making the arrest, there is no record that I know of which makes that distinction.

Nor is there any proof that the pervasive recording and dissemination of arrest records has any effect in fighting crime. In various hearings on legislation on arrest records neither the FBI nor any other law enforcement agency has presented a case that arrest records are essential in combating crime. It is more likely that the wide dissemination of arrest records has helped to create criminals,

27. *Id.* at 491.

28. See PRESIDENT'S COMM. ON LAW ENFORCEMENT AND THE ADMIN. OF JUSTICE, TASK FORCE ON SCIENCE AND TECHNOLOGY, at 216 (App. J) (1967) (Sup. Doc. No. PR 36.8:L41/Sci. 2).

29. CRIME IN THE UNITED STATES, (1969) U.S. DEP'T OF JUSTICE UNIFORM CRIME REP. 103, table 17 (Sup. Doc. No. J1.14/7: 1969).

30. *Menard v. Mitchell*, 430 F.2d at 494.

not the opposite. As Aryeh Neier, Executive Director of ACLU, has stated:

[A]rrest and conviction records often create social lepers who must exist as best they can on the fringes of society.

The dissemination of records places a series of obstacles in the path of persons who wish to enter society's mainstream and end the half-life of the world of crime. Is it any wonder, then, that recidivism rates should be so high? How can we seriously hope to reduce crime if we disseminate records which have the unintended effect of making it impossible for people to stop being criminals?³¹

Arrest records and conviction records are more widely disseminated in the United States than any other country in the western world, and yet the increase in crime in this country dwarfs by far the crime in any comparable nation.³²

The severe and devastating impact of arrest records on the right of privacy and on other rights guaranteed by the Constitution of the United States is clear. Even if these entries were essential tools for fighting crime, the wreckage of our constitutional system is too high a price to pay. However, there is no such competing consideration, and it is more likely that the wide dissemination of this information causes more crime than it prevents.

In summary, there are grave dangers to civil liberties — especially the right of privacy — posed by computerized information systems. The history of what this government has done to its citizens is enough to confirm that the potential dangers are not mere speculation.

The destruction of civil rights cannot be justified in the name of law enforcement. As Justice Brandeis said:

[I]t is . . . immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.³³

31. Statement of Aryeh Neier, Executive Director of the American Civil Liberties Union on a bill to control the collection and dissemination of criminal justice information. *Hearings on S.2008 Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 94th Cong., 1st Sess. 235 (1975) (Sup. Doc. No. Y4. J89/2: C86/16).

32. *Id.*

33. *Olmstead v. United States*, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting) (footnote omitted).