48318

PANEL — THE ISSUE OF SECURITY AND PRIVACY

Dr. Robert R. J. Gallati, Panel Moderator
Director
New York State Identification and
Intelligence System

We all recognize that the issue of security and privacy is controversial. We (the SEARCH Security/Privacy Committee) have been controversial since the day we began. What is interesting, however, is that some of the things that were highly controversial just about three years ago have already been pretty much accepted today by everybody as the way to go. And I hope that some of our far out suggestions on this panel today will be received in the light of our previous experience.

I was very impressed by Congressman Wiggins' keynote speech as I am sure we all were. He mentioned that our quest in a democracy is for a free and orderly society, and the challenge of democracy is determining how much of each we can accept. The justices, of course, are a matter of dynamic equilibrium, balancing personal liberties against individual control. Into this delicate balance we in SEARCH, and we in law enforcement and in criminal justice, have recently added the weight of technology, largely to increase the effectiveness of our control. We need to do that to be sure, but by the same token, we need to extend our concerns to political, legal and social efficiency of the counter-balancing concern for individual liberty and particularly personal privacy. And it is within this context that we would like to offer to you the wisdom of our panelists today.

The panel was designed with the logic of providing an international oversight in terms of the view from the United Kingdom, the perspective of the state and local governments, perspective of the Federal Government, and, finally, the perspective of the United States Congress.

PANEL – THE ISSUE OF SECURITY AND PRIVACY

PANELISTS

MARK GITENSTEIN
ASSISTANT COUNCIL OF THE COMMITTEE OF THE
JUDICIARY SUBCOMMITTEE OF CONSTITUTIONAL RIGHTS

DAVID MARTIN
SPECIAL ASSISTANT TO THE SECRETARY OF HEALTH,
EDUCATION, AND WELFARE AND EXECUTIVE DIRECTOR
OF THE SECRETARY'S ADVISORY COMMITTEE ON
AUTOMATED PERSONAL DATA SYSTEMS

JAMES P. MILLER
DIRECTOR OF THE POLICE NATIONAL COMPUTER
PROJECT
HOME OFFICE AND SCOTLAND YARD
UNITED KINGDOM

DONALD A. MARCHAND
RESEARCH ASSOCIATE
INSTITUTE ON LAW AND URBAN STUDIES
LOYOLA UNIVERSITY LAW SCHOOL, LOS ANGELES

THE ISSUE OF SECURITY AND PRIVACY

Mark Gitenstein
Assistant Counsel of the Committee of the
Judiciary Subcommittee on Constitutional Rights
Washington, D.C.

It is a great honor for me to have the opportunity to address you today and to represent the Subcommittee on Constitutional Rights at this symposium.

At the outset, I would like to relay Senator Ervin's deepest regrets that he is unable to be with you. It is indeed unfortunate that he cannot be here to participate in this dialogue on the critical issue of personal privacy and computerized criminal justice information systems.

Dr. Gallati has asked me to address myself to the recent activities of the Subcommittee and of Senator Ervin in the area of criminal justice information and intelligence systems. I will attempt to be as brief as possible for I am more anxious, as a representative of a Senate Subcommittee which may have a real impact on the future of such systems, to provoke questions and discussion from the audience on what we have been doing and what you think we should or should not do in the future.

There are three specific subjects which should be of interest to this panel and the symposium. First, there is the Subcommittee's government-wide survey of Federally-operated and sponsored criminal justice information and intelligence systems.

The second point is the pending legislation, S. 3834 and S. 2546, which Congressman Wiggins talked about yesterday. And a third area, which should be of great interest to you, is Senator Ervin's controversial rider to the Federal Bureau of Investigation's appropriations bill which restricts FBI dissemination of arrest records to non-criminal justice agencies.

I will cut short my discussion of the survey because I think Dave has really highlighted our work in that area. We are surveying everything the Federal Government is doing in the automated data processing area, not just in the criminal justice field – everything. The survey has already resulted in a 2,000 page hearing record which is available at the Government Printing Office and I suggest that you get a copy of it if you are interested.

This study will result in at least two important developments in the near future. First, the committee is preparing a report summarizing its findings and recommending Federal legislation. The legislation will cover all data banks operated by the Federal Government, not just criminal justice data banks. But second, and I think of greater importance to you, is the fact that Senator Ervin is also interested in separate legislation in the criminal justice field as it concerns privacy and data banks. I think you can expect to see, in the next few months, the introduction of a bill and hearings on arrest records; and, possibly, it will also address itself to other questions such as: Who shall maintain management control over criminal justice identification record systems and the more fundamental question of whether to computerize criminal justice intelligence systems.

This leads to the second general subject I would like to discuss with you and that is other legislation which is already pending. As I have suggested, I am going to restrict my comments to two bills introduced by the Administration. But before going into that I would just like to review for you the present state of Federal law on this question. For all practical purposes, NCIC and the LEAA sponsored state systems are not subject to strict Federal statutory regulations. While, of course, in some states state information systems are covered by state law, the nation-wide exchange of state information contemplated by NCIC cannot be controlled by one state statute.

The only Federal statute which is related to criminal justice information systems established by the Justice Department is Section 534, Title 23, of the U.S. Code. This statute, however, is not designed to cope with new computerized information systems, much less a system which spans the entire nation and contains, potentially at least, all the criminal justice information held in files anywhere. Indeed the central problem with the provision is that it delegates all responsibility for establishing privacy guidelines for such systems to the Attorney General. As Senator Ervin has remarked so often, "The questions of civil liberties and personal privacy simply should not be left to the self-restraint of the Executive branch."

Of course, pursuant to the authority of Section 534, the FBI has established a number of automated and manual criminal justice information systems which have been invaluable to Federal, state and local law enforcement officials around the country. For example, the Bureau's huge fingerprint identification service was established pursuant to this provision, as was NCIC. Of course,

the Bureau has made a serious effort via regulation to control the dissemination of the information it gathers and to protect the personal privacy of the subjects in its files.

However, two events in the past few years have prompted interest on Capitol Hill in Federal legislation which would establish a national personal privacy policy in regard to criminal justice data banks. The first was Project SEARCH, of which you are all aware. Through the work of Dr. Gallati and the members of the Privacy and Security Committee of SEARCH, Congress and the public have become aware of the potential threat to personal privacy posed by such systems. So in 1970, when the authorization for LEAA came up in the Senate, Senator Mathias from Maryland proposed an amendment, which was ultimately adopted, requiring the Department of Justice to submit to Congress legislation which would articulate a national privacy policy for LEAA sponsored data banks. This provision prompted the Department to introduce S. 2546, the bill that Congressman Wiggins talked to you about yesterday.

I won't go into the details of the bill because I assume that the Congressman referred to them. In general, it sets out regulations as to the type of information that may be contained in these data banks. While it does not restrict the dissemination of information to criminal justice agencies, it does only permit dissemination for law enforcement purposes. The bill also contains provisions for allowing the subject to view and challenge. It also requires updating and purging of the system and creates a civil remedy against state and local officials for misuse of criminal justice information.

The second development, which has prompted legislation, was the decision of *Menard* v. *Mitchell* by the District Court for the District of Columbia. On June 15, 1971, that court handed down an opinion which, as many of you know, has had a very significant impact upon the FBI and the whole criminal justice community. The court issued a ruling prohibiting the FBI's dissemination of arrest-fingerprint records to non-law enforcement agencies. The decision, based upon an interpretation of Section 534 almost brought the Bureau's huge fingerprint operation to a standstill. However, within a few months Senator Bible succeeded in attaching a rider to a supplemental appropriations bill reversing the *Menard* decision. This year a similar rider was attached to the Justice Department's appropriations bill by Committee. Senator Ervin convinced the Senate to amend the rider when the bill reached the Senate floor, thereby re-instating the *Menard* rule. So the second administration bill, S.3834, was introduced this summer in response to *Menard* and would amend Section 534 to place certain constraints upon dissemination of criminal records by the FBI. This bill, which has been referred to our Subcommittee, clarifies the Attorney General's authority under 534 to establish in the FBI criminal record, information and identification systems. It also establishes important limitations on the dissemination of this information as well as creating a civil cause of action.

I have pointed out these two bills because they touch upon almost every issue involved in the criminal justice data bank-privacy areas and, second, because the bills enjoyed the prestige of Administration endorsement and support.

Since our Subcommittee will probably at some time have to make a decision on these or similar bills, it would be invaluable for me to get opinions of the members of the panel and the audience on these bills and the issues they raise. For example: Do these bills still leave too much discretion on the part of the Attorney General and in LEAA to formulate policy guidelines? Can more specific standards for privacy be articulated in Federal legislation? Should Federal legislation which articulates more specific guidelines only relate to Federal agencies or should it also apply to Federally sponsored systems on the state level?

One final subject which I would hope to hear discussed today is Senator Ervin's rider to the FBI appropriations bill. For purposes of discussion it might be easiest for me just to read to you the language of the rider and to explain to you the status of the legislation and Senator Ervin's reasons for proposing it. As you might have already guessed, Senator Ervin agrees with the decision in the *Menard* case. In his view arrest records gathered by the FBI should not be disseminated to non-law enforcement agencies. Indeed, Senator Ervin has stated on a number of occasions that he can see no valid use whatsoever for an arrest record which does not contain a disposition. In that context, when the FBI appropriations bill came out of Committee this year with the Bible rider which had the effect of reversing *Menard,* Senator Ervin moved to have the rider stricken. However, he and Senator Bible reached a compromise which was adopted unanimously by the Senate.

The first part of the rider simply re-authorizes the FBI to disseminate arrest records to banks or officials of state or local governments. Senator Ervin's amendment simply limits dissemination to

these organizations by forbidding the FBI from furnishing, and I quote: "Any identification or other record indicating that any person has been arrested on any criminal charge or charged with any criminal offense, unless such record discloses that such person pleaded guilty, or *nolo contendere,* or was convicted of such charge or offense in a Court of Justice."

The FBI appropriations bill with this amendment is still pending in House-Senate conference and no one knows whether the conference will drop the provision. But there is a decent chance that it will become the law of the land and, even if it does not, I would not be surprised to see Senator Ervin propose a similar provision in future Congresses and convince the Senate to pass it again. What I am saying is, that people in the criminal justice data bank business are eventually going to have to contend with a provision like this and I am anxious to hear your reaction to this provision so that I might communicate it to the Subcommittee and to Senator Ervin.

Before concluding, I would like to make one very important clarification about the Senator's position on privacy and computers. He is aware that many of the decisions that he makes on these issues are not exactly well received by those involved in establishing governmental data banks and by the technologists who design and operate them. He realizes that privacy and security safeguards undermine the efficiency and increase the costs of computer systems. But, as Senator Ervin is fond of saying, "If we want to have a free society we must take some risks."

THE ISSUE OF SECURITY AND PRIVACY

David B. H. Martin
Special Assistant to the Secretary of
Health, Education and Welfare and
Executive Director of the Secretary's
Advisory Committee on Automated Personal
Data Systems
Washington, D.C.

I am going to tell you a bit about the origins and purposes of the Secretary's Advisory Committee on Automated Personal Data Systems because I think it is not the most notorious activity that is happening under the banner of HEW.

The single social phenomenon that can be most credited with having given impetus to the creation of the Committee was the hearings of U.S. Senator Sam J. Ervin's Subcommittee on Constitutional Rights in the winter of 1971, which, as I am sure most of you realize, provided a forum for many institutions and individuals of America to express their concern about certain forces that seem to be at work in our society. Although most of us would probably agree that we do not well understand what these forces may be, we would also agree that there does seem to be considerable malaise about these forces -- a malaise that was manifest in much of the testimony which Senator Ervin elicited through those hearings; a malaise that has also been stirring in England, France, West Germany, the Scandanavian countries, Canada, Japan and Australia. Something is tickling the discomfort button of citizens in all these countries about the onset of a technology which they do not well understand and whose social implications are far from clear to them.

The Secretary of Health, Education and Welfare, Elliot L. Richardson, was invited among many other persons to testify before the Ervin Subcommittee. The subject matter that the Subcommittee was especially interested to have the Secretary address was the use of the Social Security number, an element of technology that was created in 1936 to facilitate the administration of the social insurance program enacted on August 14, 1935, in the Social Security Act. The Social Security number started out being an element of technology for the sole use of the Social Security Administration. Its utility, however, as a means of helping to sort information accurately to the records of a large number of persons, many of whom have identical or similar names, became evident to many others. On the initiative of the Civil Service Commission in 1943, President Roosevelt was prompted to issue an executive order mandating that the Social Security account number should be used by all other Federal agencies as the means of organizing individual account records. The executive order was not instantly carried out and has not been fully adhered to. But gradually most agencies of the Federal Government that have had large-scale individual record-keeping requirements have come to use the Social Security number. So have many other organizations in society, both in the private sector and in State and local governments. And citizens have become aware of the fact that this element of technology has spread and as a consequence have been led to wonder about the significance of its spreading. Many have assumed that there is some kind of harm or disadvantage lurking in the weed-like spreading of the Social Security number.

So the Secretary went to the Ervin Subcommittee hearings and discussed the Social Security number and the ways in which the Social Security Administration has administered its data bases, both its computerized and non-computerized data bases. In the course of his exchange with the Subcommittee members, the Secretary indicated his intention to establish an advisory committee for himself and the Department. It was not clear at the time he testified what the task of such a committee would be. In March, 1970, the Social Security Administration, in part to respond to a proposal made by the American National Standards Institute (ANSI) that the individual's name and Social Security number be made the standard form of identification of individuals for purposes of data interchange, had established a task force of its own officials known as the Social Security Number Task Force. This group was charged with reviewing the policies and practices of the Social Security Administration relating to the Social Security number and making recommendations about them to the Commissioner. The Task Force concluded that there were several social policy issues relating to use of the number by organizations outside of the Government that are beyond the reach of the Social Security Administration and recommended that the Secretary create a public advisory body to examine and advise about these issues.

The officials of the Social Security Administration were primarily interested in issues of Social Security number policy. It took many months of discussion by a number of us who were considering what tasks such an advisory committee should undertake to conclude that it would not serve any very useful purpose to commission a group to advise the Department solely on what to do about the Social Security number. We recognized that if one thinks of the Social Security number as an element of technology useful in the mangement of records, and adopts the most conservative policy with respect to the use of the Social Security number – that only the Social Security Administration should use the number – one would not even begin to address the problems that people are concerned about relative to the application of computer technology to record-keeping. We concluded that the Social Security number is just a proxy for other sources of concern and that there is very little you can say about the use of the Social Security number itself that addresses those other sources of concern. With the recognition that the task had to be broader than Social Security number policy, we developed terms of reference for the Advisory Committee as follows:

1. to analyze what the potentially adverse consequences are of applying automated data processing technology, coupled with communications technology, to data bases that include identifiable personal information;
2. to analyze what safeguards might be developed to protect against those adverse consequences; and
3. how one might implement such safeguards.

The task, as the Advisory Committee has been discovering since it started work last April, is much broader than individual privacy.

The Advisory Committee is scheduled to deliver its report to the Secretary by the end of this year. It has not fully decided how it feels about the issues with which it has been dealing and it has not yet crystalized fully its recommendations, but even if it had it would not be appropriate for me to be the person to share these with you at this time. Speaking personally, I would like to suggest that undue concentration on the issue of individual privacy, or of confidentiality of information, however important it is, leaves us at peril of ignoring some much broader, more substantial, perhaps, more troubling issues. Records and record-keeping have been with us for centuries and the problem of individual privacy is a function of how one maintains records, how one shares records, how well one secures them or does not, and what incentives there are for dishonest or malevolent people to make inappropriate use of records. This problem has been with us for as long as we can remember in history; for as long as we have been able to make records in whatever form for whatever purposes. The computer does certainly add a new dimension to this problem. It is not clear whether there is a net loss or a net gain. There are lots of ways in which the new technology makes it possible, more easily than without the technology, to assure certain states of privacy and there are other aspects of the application of the technology that enhance the risks to privacy.

I would like to appeal to you all as individuals to consider the broader issues. First, as it seems to many of us who have worked in this area, the combined application of computer and communications technology to record-keeping holds potential for some effects, whether for good or bad is for someone else to say, on institutional autonomy and institutional pluralism. Many members of this particular audience nourish the hope, maybe the belief, and surely indulge in the rhetoric, that the National Crime Information Center is a State-controlled system and that the State participants in the system are losing no autonomy out of the arrangements that are facilitated or necessitated by the technology. I have heard Inspector Roderick, who is in charge of NCIC at the F.B.I., say from his standpoint that the F.B.I. does not really run the NCIC; it is just a kind of holding company for the States.

Now, whatever the accuracy of these perceptions may be today, whatever the merit of such hope may be today, it seems to me that one can predict with some confidence that one consequence of applying computer technology to that kind of a system is going to be to erode bit-by-bit the autonomy of its participants and to fuse them increasingly under central direction from Washington. Whether that would be good or bad is another question, but as an outcome, if my hunch proves correct, it would be an effect of the technology that some people might be very concerned about.

A presentation by Harold Greene, Chief Judge of the Superior Court of the District of Columbia, was made at the September meeting of the Advisory Committee in which he spoke firmly and eloquently for the proposition that if the courts are going to have computerized information systems they had better be owned and managed by the courts. They should not be in the control or management of the Executive Branch. He was making a plea for institutional autonomy. He made it very clear. He said the judiciary is an indepen-

dent operating branch of government and it will either lose a degree of autonomy and capacity for impartiality in doing the job expected of the courts or it will *appear* to lose it in the eyes of litigants if court computerized information systems are set up under the control and management of the Executive – in the case of Judge Greene's court, the Justice Department. Under such circumstances, said Judge Greene, criminal defendants would believe that the courts are part of a monolithic enterprise involving the prosecution and correctional institutions.

Those of you who read the papers currently may have noted that BART, the new public transportation system for the San Francisco Bay Area in California, within a few weeks of its inception in operation, had a failure in its computerized controlled braking system. The newest and "safest" mass transportation system has already, within a few weeks of coming on the line, had an accident in which five people were hurt. The comment on the first wave of the story, and I haven't seen more, was, "We don't know what happened." People who are students of large-scale systems say about them that by the time a system has been designed and implemented through a year or two or three of work, there are very few people, if any, that understand how it works, what it is all about, or how to adjust or change it readily if something goes wrong.

If our social operations become significantly dependent on large-scale computerized systems, we are building a new source of risk of their discontinuity of function. This may be all right. We are going through this sort of risk every day, but we ought to be aware of it and it is a risk that I think we can only overcome by enormous attention to questions such as: What is the objective of the system? Is it worth doing? Is it worth making so big? How should we design it? What sort of safeguards should we build in?

Technology has a way of just coming on. Technologists are not going to stop. They are "doing their thing" every day. We are on a computer binge in this country and throughout the free world and top management isn't watching. Today's management is by and large ignorant of and a bit put off by computers. It doesn't understand them. It doesn't want to have to get involved with them. And so the technologists are effectively in charge. The history of man's use of technology is that it takes the rest of us, who are not technologists, to put social controls on technology to curb its potential for harm. I don't say this in any way unkindly about the technologist – the rest of us agree, we wouldn't be able to do a lot of the things we are able to do now without technology in all sorts of fields. But the rest of us typically don't wake up to the significance and social implications of a technology until its adverse effects are so much with us that we just can't escape noticing. And then we have a very difficult task of undoing or modifying or correcting the effects of technology that we don't like.

Perhaps there will be a chance for discussion to add a few more comments about broader dimensions of concern about the application of computers to personal record-keeping that aren't encompassed by what we understand by "individual privacy," and that will not be addressed by settling issues of data security and access.

THE ISSUE OF SECURITY AND PRIVACY

James P. Miller
Director of the United Kingdom
Police National Computer Project
London, England

It has been said that the greatest divisive force between the American and the British people is that they both speak the same language. On the assumption that this could apply to what we are doing on the other side of the Atlantic as compared to what you are doing on this side (and we have learned a great deal of what you are doing in the United States at this very excellent seminar), I think it might not be wasting too much time if I were to give you a very quick rundown of some of the differences between our two societies in the law enforcement field.

First of all we, are very much smaller than you. We have about 55,000,000 population as opposed to your 200,000,000 plus and we are very much smaller geographically too. We are a Unitary State and have not the problems that go with a Federal constitution. So, basically, there is only one layer of law enforcement in the United Kingdom – the local police forces of which there are something like 55 in the country. There are approximately 100,000 policemen in these 55 police forces. The only small exceptions to this general rule are a few specialized agencies such as the Railway Police, the Post Office, Customs and Excise Department and, of course, the armed forces.

The role of the Secretary of State for the Home Department (and it is not unlike the Department of Justice's role here although there are differences) in relation to law enforcement is that the Secretary of State for the Home Department has a general responsibility for law and order in the country. He pays fifty per cent of the cost of local police forces and because of this has certain rights of inspection and provides certain central services. He provides for central services in the forensic field, the police training field, and in the operational computer field. I use the word "operational" to make a distinction from the normal batch processing type of computer system which we are content to leave to the local authorities, associated with local police forces.

There is the complication of the special role of Scotland Yard which basically is the police force for the metropolitan area of London which contains about 9,500,000 people. It also has a number of national functions. For a long time it has kept the national records of crime and criminals. It provides assistance in important crime cases at the request of local police forces and it provides the anti-subversive, the special branch eleme[illegible]which I gather is mainly done by the FBI in th[illegible]ntry.

Law enforcement record systems – just a very quick and rough background would be of some interest perhaps. The first law enforcement record systems in the UK probably goes back to the days of Henry II when the governors of prisons were given the responsibility for producing lists of prisoners to the traveling justices (at the beginning of the development of the common law in fact).

The first serious attempt to record what happened to persons at trials occurred in an Act of 1821, when really the basis of the first criminal statistics, and the first central record, of criminals came about. This is still produced. It is known as the After Trial Calendar and it refers only to convictions at Assizes and Quarter Sessions. It doesn't refer to convictions in lower courts.

The first comprehensive national record of crime (offenders rather, not of crime) started 101 years ago in 1871 when the Prevention of Crimes Act was passed giving the Secretary of State power to keep a national record of offenders. He delegated this job to the Commissioner of Police for London (or to "Scotland Yard"). Scotland Yard has held this record ever since. It was, first of all, a record of the names and descriptions of people with criminal histories and then when Commissioner Henry invented the system of fingerprint classification in the early part of this century, it became the national fingerprint record office as well.

The development from there to the computer systems has taken a long time. We are not as far advanced as many of you are in this country in this field but we have reached the stage of a complex Burroughs B6700 twinned processor system. The equipment has been delivered, is ready for action, and is being used at present for program development. It will have something like a thousand terminals attached to it – mostly, by the way, VDU (CRT's) and not dataprinters. The first operational application will be going live by about March next year. I won't go into this further at present because this is obviously not the time nor the place.

But I think you might be interested in our approach to the security of the system and, therefore, its degree of privacy. They are connected very closely, and they are not really significantly differ-

ent in the computer system from what they already are in manual systems. For a start, there are records of about 2,000,000 people in the National collection and these are, may I emphasize, of convicted persons only. An arrested person does not find his way into that collection until he has been convicted in front of a court and is regarded as a convicted person. It is only the more serious forms of offenses that are in the National Record and, without going into details, those offenses for which there is legal authority to fingerprint the offender on arrest (for what I think you would call felonies on this side of the Atlantic and the more serious misdemeanors.) Minor offenses (drunks, traffic violation, etc.) are not included in the record.

The computer installation is in a secure building in a training estate surrounded by several hundred policemen in various stages of training. Across the road from it is a Royal Air Force Base with many air force personnel. The building itself is built almost like a fortress so the actual physical security is very high indeed. The terminals that will allow access to this computer system are also in secure buildings which are manned 24 hours a day and usable only by police officers or civilian staff who have been specially cleared security-wise for this purpose.

The network is entirely, what we call, a "private" one. I think you would call it a leaseline network here. The first standby is another exclusive use network, and then, in emergencies only, the public network is used for interrogation and up-dating. Finally, of course, every single person concerned with this system is covered by what we call the Official Secrets Act. In other words, if he discloses any information he receives in the course of his official duty he is liable to penalties under the criminal law. I won't bother going into the considerable software checks that we are also putting into the system. It's for another day, probably.

Getting to the more general issue of privacy in the United Kingdom (having left the privacy and confidentiality and security of the police law enforcement computer record system) the history is a fairly recent one. It is feared in some quarters that computers will menace privacy in general.

Around 1968 the National Council of Civil Liberties produced a publication which raised the issue and at roughly the same time a group of Conservative lawyers expressed much the same fears as the National Council of Civil Liberties had done. Two Bills found their way fairly quickly on to the floor of Parliament and there were several debates. As a result of all of this a committee was set up under the chairmanship of Sir Kenneth Younger and that committee has, in fact, just reported.

The Younger Committee by its terms of reference did not look in detail at Central Government computer aspects but instead the Government set up a separate internal committee which is, I gather, about to report. The two committee reports will be considered by the Government and I would guess that fairly soon there will be a considered document, we call it a White Paper, which will no doubt be debated in Parliament and may be followed by legislation, possibly late in 1973 or in the beginning of '74. I must emphasize that this is a private citizen's view only. I have no official information on the point.

The findings of the Younger Committee are interesting in many respects. They considered first of all the philosophical issue of whether there was in fact a general right to privacy. If I may quote one paragraph from it, I think this sums up a good deal of its final attitude. It says:

> "If there were to be a right of privacy under the law it should not, in our opinion, be synonymous with a right to be let alone. An unqualified right of this kind would in any event be an unrealistic concept, incompatible with the concept of society, implying a willingness not to be let entirely alone and a recognition that other people may be interested and consequently concerned about us. If the concept were to be embodied into a right, its adaptation to the dominant pressures of life in society would require so many exceptions that it would lose all coherence and hence any valid meaning. We have concluded therefore that the type of conduct against which legal protection might be afforded on the ground of intrusion on privacy should be confined to injurious or annoying conduct deliberately aimed at a particular person or persons where the invasion of privacy is the principal wrong complained of."

The reverse of this concept (in other words, of an abstract right to privacy) hasn't been followed, I know, in other cases, and in other places in the United States too, I understand. There was a minority within the Younger Committee who took the line that there should be a general right of privacy, with the ability to sue if it were breached.

The report itself is lengthy and it ranged over a whole series of fields through broadcasting, the press, the rest of the media, the private detectives, credit rating agencies, etc. I don't think this is the time or place to go through it in its own detail.

I am reminded at this point of a story going around the United Kingdom. It is of two Irishmen who found themselves in front of St. Peter at the gates of Heaven and St. Peter asked them who they were.

They gave their names as Pat Murphy and Shamus O'Leary.

St. Peter said, "Tell us more about yourselves."

They said, "Well, we are members of the I.R.A."

So St. Peter said, "Members of the I.R.A. aren't allowed in here."

Pat said, "It's all right, your Reverence. We don't want to get in. All we are saying is that you've got ten minutes to get out."

It is clearly important, therefore, to see things from the other fellow's point of view. I think I will conclude by saying that this is the other fellow's point of view (holding up report). The cost is about two pounds. I haven't seen the *Wall Street Journal* for the closing rate today but I suppose its equivalent is about $5.00. I think if any of you are interested it might be well worth investing in it just to get the general U.K. background of thought to this most important question.

THE ISSUE OF SECURITY AND PRIVACY

Donald A. Marchand
Research Associate
Institute on Law and Urban Studies
Loyola University Law School
Los Angeles, California

Continuous population growth coupled with rising crime rates have increased the complexity and control of information-handling activities in local, county and state criminal justice agencies. In the last seven years, various criminal justice agencies have perceived the need to apply the computer to a variety of tasks, ranging from automating the administrative records of an individual agency and scheduling court activities, to such sophisticated applications as the Los Angeles Police Department's Pattern Recognition and Information Correlation System – or PATRIC as it is called – and Santa Clara County's Offender Based Criminal Justice Information Control System. As Table I indicates, the development of computerized information and communication systems in criminal justice agencies in California has assumed major proportions as indicated by the numbers of systems already operational or being planned.

Approximately 139 computerized information and communication systems are either being planned, being implemented or are currently operational in criminal justice agencies in the state. Of these systems, 8 are in various stages of development at the state level. The same is true of some 71 systems at county levels and 58 at city levels, with 2 computerized information systems serving multi-county or multi-city needs. Such totals are fluid as a result of the continuous mushrooming of new systems and the absorption of existing operations into more comprehensive entities. An example of the latter phenomenon has been the planned consolidation of some 20 different systems in Los Angeles county into a regional justice information system. Our figures then show a close approximation of what is currently in existence, and more important, what is being planned.

The development of systems is consistent with the concentration of population with the largest cities and counties initiating the more extensive and sophisticated applications. As Table II indicates, offender-based criminal justice information systems have been planned or developed in 5 counties. On the other hand, in the larger cities, priority has been given to development of what are considered to be either police information systems or partial applications such as want-warrant, arrested persons, command and control or traffic record systems. In the superior or municipal courts, the more numerous applications have been in the case indexing, jury services, and scheduling functions. The case following function is a relatively late application and has generally emerged with the offender-based criminal justice information systems. In the corrections area, systems development is less advanced except for the California Department of Corrections and Youth Authority's plans for a correctional information system and the Los Angeles County Probation Department's management and information systems.

The costs of all these applications are not as yet estimable. No one seems to know how much all this is costing the state or individual cities and counties which are bearing the major share of such costs. Ever-changing hardware, software and personnel requirements make even an educated guess hazardous. Because of the decentralized manner in which systems have developed in the state, there are no accurate figures concerning how much the statewide criminal justice information system really costs if one expands, for a moment, one's definition of such an information system to include not only the state justice department's own criminal justice information system, but also the related and, in many cases, interfacing local and county systems.

The federal contribution to systems development in California is shown in Table III. These federal funds are authorized by the Omnibus Crime Control Bill program and the Highway Safety Act program.

Since the Omnibus Crime Control Bill program began in 1968, federal funds disbursed by the California Council on Criminal Justice have totaled some $13 million with another $1 million added through discretionary grants from the Law Enforcement Assistance Administration (LEAA) to various criminal justice agencies in the state. It should be pointed out, however, that we do not know nor, so far as we can tell, does anybody know what the total costs of these systems have been. What individual agencies have provided in the way of matching funds to receive the federal grants represents only a portion of what has actually been

spent on any one system's design and implementation. Federal monies have served to accelerate the existing momentum to develop new and more extensive systems, while the California Council on Criminal Justice has been able to provide but limited direction in terms of coordinated system planning and development. The Council itself is aware of the need for greater coordination as indicated by its action at the April '72 meeting. It then resolved to be extremely critical of any new information systems at either the state or local level. In addition, any refunding of information systems would be contingent on their compatability with neighboring or state systems and further would be contingent on assurance that there would be no file duplication by any agency of information maintained within the state level criminal justice information system. Only recently has the Council sought to limit the proliferation and duplication of systems and has initiated surveys to determine how many court, police and offender-based systems exist and to further develop plans for consistent and controlled growth.

Since 1965 some $3.5 million of federal traffic safety money has supported the development of about 29 systems, primarily concerned with traffic court and traffic record systems. Although these are related to criminal justice information and police information systems, little coordination exists between either state planning agency. While the Council on Criminal Justice and the Office of Traffic Safety have liaison persons, systems development has occurred independently.

Federal funds then have contributed substantially to the criminal justice system development picture in California. Some $17.5 million have been allocated with larger grants yet to come. If coordinated and planned efforts are necessary, they must be initiated soon if further proliferation and duplication of systems is to be curtailed effectively.

Administrative policy concerning the use of electronic data processing and the protection of privacy and security in California has gone through various stages. California has shifted its administration for EDP use several times during the last seven years. Although masterplans for the utilization of EDP have been issued, the organizational structures have not as yet been stable and enduring enough to implement them. Responsibility for the management of EDP at the state agency level has been shifted from the Office of Management Services under the general supervision of the Lt. Governor to the Systems Control and Development Section of the Department of Finance. While the state has consolidated all its EDP services into 4 data centers, it does not now control and coordinate the uses of EDP by criminal justice agencies at the city or county levels.

In 1968, the Intergovernmental Board on Electronic Data Processing received statutory authority to coordinate the development of intergovernmental information systems and to establish guidelines and criteria to safeguard privacy and security. Since its initiation, the Board's resources have fluctuated from a high in 1969-70 of $63,000 to a low in 1971-72 of about $10,000. Just recently, the Board reacquired an executive secretary and is ready to begin again with a 1972-73 allocation of some $30,000.

Thus, lacking statewide guidance and with independent responsibilities, the city and county criminal justice agencies have initiated their own systems to meet their specific needs. From the perspective of systems operation, the California experience may be characterized as follows: state level systems have developed with limited coordination with city and county applications. City and county systems in turn often reflect parochial planning or duplication with limited interface capabilities between state or similar city and county systems. The result is uncoordinated growth of numerous systems at immense and incalculable public expense.

What, then, of privacy and security considerations in California? At the state level there has been coordination and consolidation for the use of EDP. Privacy and security considerations have been left generally to the individual state agencies, including the state Department of Justice. These agencies all have management control over their systems, including responsibility for development of privacy and security regulations. These, in turn, are subject to review by the Department of Finance. To date, privacy and security considerations have received limited attention or official agency commitment. While security regulations have, for example, been developed for the State Justice Department's criminal justice information system, privacy and confidentiality considerations have not as yet been formulated.

Two county systems, Santa Clara and Los Angeles county, have used project SEARCH guidelines and adopted codes of ethics. Apart from such individual efforts, little more has been done. The intergovernmental board on electronic data processing, to date, has contributed very little to the development of intergovernmental guidelines.

No research efforts or studies have attempted to treat the problems peculiar to California's immense criminal justice information system.

As far as legislative initiatives concerning privacy and security go, several bills have been proposed which have tried either to adopt the project SEARCH model state act or selected sections of it to the California situation.

In April, 1971, an assembly bill was drafted to create a security and privacy council, appointed by the Governor, in order to "conduct a continuing study and review of questions of individual privacy and security in connection with the collection, storage, dissemination and usage of criminal offender record information." The bill proposed to adopt the project SEARCH model state act to fill the apparent gap in the state Justice Department's handling of privacy and confidentiality concerns. The bill was opposed by the State Department of Finance on the grounds that it was premature and a too literal application of the model act to the California situation. It died in committee.

In March, 1972, a second assembly bill proposed creation of a criminal record dissemination board to conduct continuing study regarding the dissemination of criminal offender records information to non-criminal justice agencies. The bill also defined what minimal data elements constitute a criminal offender record, stipulated that intelligence and investigative reports not be included, that access to such records be limited to criminal justice personnel on a need-to-know basis and that reporting of such information be made more uniform and efficient throughout the state. The bill is currently pending before a state senate committee.

In addition, a third assembly bill also proposed in March, 1972, required the attorney-general to assure the security of criminal offender record information from unauthorized disclosure at all levels of operation in the state; to make sure that such a record be disseminated only on a need-to-know basis; to coordinate the latter activities with interstate systems; and to initiate a personnel educational program concerning the use and control of criminal offender records information. Also, the bill would require each agency holding or receiving criminal offender record information to maintain a listing of the agencies to which it has been released: this bill is pending before the same committee.

If the latter two bills are passed, California will have taken a first and much needed step. In the absence of such legislation, existing state regulations are a patchwork of state codes applicable to public, juvenile and adult criminal records. In November, 1971, the Governor signed into law a bill providing for the individual the right to review his record contained in the State Justice Department's information system for errors and omissions. While this is a step forward at the state level, no equivalent legal right is available at the county and city level where the issue is contingent upon the option of system management.

The problems are indeed complicated. Our legislature is just beginning to grapple with the issues. For example of unresolved problems: interfacing requirements and safeguards among intergovernmental systems; standards regarding data maintenance and dissemination; and difficult policy questions concerning whether, when and how to close, seal or purge records.

To summarize: the California experience is a dynamic and multifaceted one. Presently, the development of adequate privacy and security safeguards has been outpaced by the development of computerized information and communication systems in the criminal justice agencies in California. The two processes, in my estimation, must be compatible and become one. California, as a leader in the field of automated criminal justice information systems, shows consistency in this area of growth as in other aspects of its development. We have more of everything than we are currently able to keep track of, account for, or regulate. How large a gap in timing before coordination and development of essential safeguards takes place is at this time uncertain.

TABLE I

STATE OF CALIFORNIA

COMPUTERIZED CRIMINAL JUSTICE INFORMATION AND COMMUNICATIONS SYSTEMS:

CUMULATIVE LISTING

STATEWIDE	8
MULTI-COUNTY	1
COUNTY	71
MULTI-CITY	1
CITY	58
TOTAL SYSTEMS	139

TABLE II

STATE OF CALIFORNIA

COMPUTERIZED CRIMINAL JUSTICE INFORMATION AND COMMUNICATIONS SYSTEMS:

APPLICATIONS

	Offender-Based Systems	*Law Enforcement Systems*	*Court Systems*	*Corrections Systems*
STATE	1	6		1
MULTI-COUNTY		1		
COUNTY	5	27	32	7
MULTI-CITY		1		
CITY		54	4	

TABLE III

STATE OF CALIFORNIA

COMPUTERIZED CRIMINAL JUSTICE INFORMATION AND COMMUNICATIONS SYSTEMS:

FEDERAL CONTRIBUTION

I. OMNIBUS CRIME CONTROL BILL PROGRAM

A. ACTION GRANTS (California Council on Criminal Justice)

TOTAL SYSTEMS FUNDED 30 — TOTAL ACTION GRANTS $13,091,700

B. DISCRETIONARY GRANTS (Law Enforcement Assistance Administration)

TOTAL SYSTEMS FUNDED 6 — TOTAL DISCRETIONARY GRANTS $ 998,508

TOTAL CONTRIBUTION THROUGH OMNIBUS CRIME CONTROL BILL PROGRAM $14,090,208

II. HIGHWAY SAFETY ACT PROGRAM
Business and Transportation Agency, Office of Traffic Safety)

TOTAL SYSTEMS FUNDED 29 — TOTAL CONTRIBUTION THROUGH HIGHWAY SAFETY ACT PROGRAM $ 3,426,576

III. SUMMARY FEDERAL CONTRIBUTION

A. OMNIBUS CRIME CONTROL BILL PROGRAM	$14,090,208
B. HIGHWAY SAFETY ACT PROGRAM	3,426,576
COMBINED TOTAL FEDERAL CONTRIBUTION	$17,516,784

END