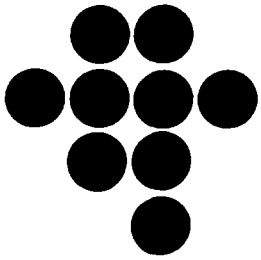

COMMUNICATIONS
FORUM

RECENT DEVELOPMENTS IN NATIONAL INFORMATION SYSTEMS: A DOSSIER SOCIETY

Kenneth Laudon, New York University
Sanford Sherizen, Information Security Consultant,
Natick, MA.
Gary T. Marx, MIT

April 24, 1986

Genga Arulampalam, Rapporteur

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Massachusetts Institute of Technology
Communications Forum

RECENT DEVELOPMENTS IN NATIONAL INFORMATION SYSTEMS: A DOSSIER SOCIETY

Kenneth Laudon, New York University
Sanford Sherizen, Information Security Consultant, Natick, MA.
Gary T. Marx, MIT

April 24, 1986

Genga Arulampalam, Rapporteur

RECENT DEVELOPMENTS IN NATIONAL INFORMATION SYSTEMS: A DOSSIER SOCIETY

Kenneth Laudon - New York University

Laudon based his remarks on his book titled 'The Dossier Society' (Columbia University Press). This book is the result of 6 years of effort and is due to be released in June this year. In introducing the lecture as well as the title of his book, Laudon pointed out that the key idea of America originally, was to free people from all types of unlimited surveillance. The genius of American politics he said, was to fractionalize the various powers/authorities: executive, judicial, and legislative. However, he asserted that with the development of telecommunication, computer hardware, and related software, it is now possible to put these fractions of power together without a constitutional convention. The thesis of his book he said, is that there has been a steady errosion in the organizational principles which make America a democracy and instead there is a movement towards a different kind of social order which he called a 'dossier society' (DS).

Laudon then listed and briefly described the various facets of the DS:

1) Individual - decisions made on the basis of data images and data trails in various databases, not face-to-face interactions or thorough analysis or understanding of the case.
2) Technical - emergence of integrated files and the development of central national files.
3) Political - unprecedented concentration of power and authority.
4) Sociological - widespread social surveillance.
5) Cultural - many people have an 'official life', existing on record systems in various locations.

He considered the DS to be a difficult reality to describe partly because it is an emergent reality; it is not here yet. As an example of national information systems he mentioned the files maintained for the following groups of individuals: 95 million tax-payers, 24 million criminal fingerprint records(with the FBI), 60 million civilians in a huge registered vehicles file. These information systems are national in scope, very large (millions of records), complex, and centralized.

Information files at the local, state, and federal levels can now be integrated functionally and jurisdictionally (medical, welfare, taxation, police, etc.). Laudon said that technology cannot be blamed as the sole cause for the emergence of these systems. Some of the major forces behind the development of these systems are:

1) bureaucratic - national information systems are sometimes budgeted at 500 million to over one billion dollars, spent over 5-10 years (major budgets and political

patronage involved).
2) political I - information systems being used as a solution for problems that really don't have a solution.
3) political II - while ideologies of both liberals and conservatives differ, both sides for different reasons strongly support the development of very powerful national information systems.
4) social/cultural - there are very few social problems that don't have a computer recommended as a solution.
5) technology - information from isolated files are brought to bear in situations far from the context in which it was gathered (this is directly opposed to the organizational principles of democracy)

Laudon stated that privacy now takes on a new meaning. Unlike the 'routine-use' clause in the Privacy Act of 1974, the current administration asserts that there is a generalized government interest in any information that happens to be in the federal domain. This is the current legal doctrine which supports the rapid development of national information systems. In addition to the constitutional and legal issues, Laudon briefly discussed the functional issues(value and workability), political institution issues(role of the federal government, accountability of Congress, and incrementalism in policy), and social issues (impact on organizations, impact on public values, and relationships between key groups).

Laudon then discussed his intention in 1978 to investigate and study the national information systems which consist of the FBI, IRS, and SSA. Subsequent volumes will focus on the SSA and IRS. The FBI's computerized criminal history system(CCH) is very complicated and contains millions of records. These records are basically histories of arrests, convictions, etc, which are used by police, courts, and correctional institutions at the local level. Laudon used a slide to show a sample criminal history record of which the system has approximately 24 million. He stated that these files were requested approximately 7 million times in 1980 and over half the requests were non-criminal- justice related - for employment purposes. He further pointed out that 40 million people in the US have a record of arrest. The system as it exists in 1986 is comprised of two databases - one, the fingerprint file with records of 24 million people and the other the name index with 30 million names in it(and no fingerprints). He described the procedure used by requesting agencies, such as police officers on duty, who call up information from the criminal history index via the national criminal information center (NCIC) computer to find out whether a particular name is on file. If the name is on file it helps them arrest the individual and subsequently verify the details of the previous arrest which may have even been a situation where the case was dismissed. Laudon stated that a close look at the criminal information system shows that it is comprised of 3 parts. First, the criminal justice system, next the national employment screening system and finally the national identity center, with the FBI as the central coordinating body.

In order to study these systems Laudon conducted 120 interviews at the 'street level', talking to police, criminal court magistrates, etc,. He also did a 50 state survey, a data quality audit (which is the first independent audit of this nature) and lastly a social impact study to investigate the adverse effects of this system.

Laudon discovered that approximately 55% of all federal use and 25% of all state use of this system is employment related. At the state level it is being increasingly used for employment purposes, and he anticipated that it would soon replace the criminal justice use as the most important. The people who are checked with this system (according to the American Bar Association) includes 7 million state licensed professionals such as doctors, lawyers and barbers, and 15 million government workers at all levels. A negative side to this, pointed out by Laudon, was that a record of arrest (even without conviction) was sufficient to deny employment. He noted that the pressures causing an increased use of these systems for employment purposes were an increase in crime rate, state centralized records(e.g.for employment of meter readers), vanishing constitutional protections, and liability pressures on employers. Discussing data quality, Laudon said that of the NCIC files, 55% of those sampled were found to be incomplete and ambiguous with several serious errors. In addition, from the FBI's wanted persons file, 12,000 erroneous warrants are issued everyday. As part of his study, Laudon looked at the federal regulations related to the use of these files - primarily an individual's rights to inspect, challenge review, limit dissemination, 'purge & seal', and management's responsibility to hold complete and accurate information, audit local users, and maintain transaction logs. However, he observed that very often neither an individual's rights nor management's responsibility were properly executed. The last area of his study was the investigation of the social impact of the FBI's criminal history system. While there are several facets to the social impacts, Laudon focussed his attention on 3 aspects - organizational decision making, group and institutional relationships, and social values. In the area of organizational decision making Laudon observed that while the system was thought to be a powerful tool, at the local level criminal justice people(police, magistrates, etc.) were not interested. On the other hand, non-criminal justice people such as employers and defense department contractors expected the system to have a powerful effect in their area. As for group and institutional relationships, Laudon observed the negative impact of this system in the welfare of sub-groups, and also there arose questions of balance within the criminal justice system. Laudon pointed out that from a social value point of view, the system had no impact on effective criminal justice while at the same time it posed problems of accountability, constitutional protection, public trust in government, and potential for abuse.

Laudon mentioned that the FBI system had several options open to it, both from a technical point of view and a

policy point of view, to reduce the significantly large negative impact it had at present. On the technical side he cited three options which though not as effective as the policy options still could be used to improve the system. The technical options are:

1) 50 separate filing centers one in each state without central control.
2) a clearing house type of system.
3) a central library.

The policy options are:

1) file size - narrow bandwidth instead of the present wide bandwidth.
2) file content - index vs full record.
3) data quality - status quo vs new legislation.
4) dissemination - single file vs dual file (arrest and conviction separate).
5) control - state vs federal.

In closing Laudon asserted that the FBI system as it exists today is a billion dollar system, which since it is totally controlled by the FBI poses problems of gargantuan proportions - effectively a 'run-away' system. He also stated that the reason for public policy failure was due to the lack of basic research, bureaucratic politics, and shoddy development practices.

Sanford Sherizen - Information Security Consultant, Natick, MA

Sherizen's lecture focussed on the privacy and security issues related to the national information systems. He indicated that Prof. Gary Marx and himself had recently completed a draft rreport for the US Congress, Office of Technology Assessment (OTA). This report examined the privacy and security implications of work monitoring. A report from the OTA will be rreleased to the Congress in the Fall and be available to the public at that time.

He asserted that in many situations "yesterday's technological development is today's social problem". He said that from the point of view of privacy and security the old answers don't work in today's context. i.e. many of the driving factors of the Privacy Act of 1974 are not appropriate today. He claimed that we are in a situation where those who are developing the tecnnology and those develping the legal and/or moral issues don't understand or relate appropriately. As a result we have very advanced information sytems but people are not asking the right legal or moral questions -"are we better-off or not?". Due to the complication of information technology and the lack of creative use of that technology, police today he said, are less effective than in tne "old days", inspite of the fact that billions of dollars have been spent in an attempt to improve the information systems.

Sherizen pointed out that in addition to the 3 national information systems referred to by Laudon there are several other information systems (databases) being developed for public use, and adequate thought was not being given to its impact on people's privacy and security. As an example of the complications of determining appropriate privacy, he cited the database developed for use by doctors to find out which patients have have sued doctors in the past. An alternative system was then produced to help patients choose doctors who have not been sued. Sherizen said that public information stored in such advanced information systems as we have today have far reaching effects and he emphasized the need to investigate thoroughly the resultant implications before embarking on or accepting such systems for daily use.

He said that in the past one could through a tedious process gather information about an individual. However, today a business could call TRW for credit information on 120 milliom Americans or one can obtain this information in a number of other ways much easier than before and without going through a whole paper trail. Also he pointed out that this whole process was quite legal. He quoted David Burnham (New York Times) as saying that the US government has 4 billion separate records on US citizens. Sherizen stated that though people should be asking questions about their own privacy, at present very few do so and there are no mechanisms that allow such questions to be addressed. A recent issue - the urine analysis issue - suggested by the President's Commision on Organized Crimes, he said, has caused a lot of discussion/debate within the context of privacy and security. However, he expressed surprise at the lack of historical knowledge of those involved in the discussions. Sherizen said that in such cases most often the issue begins with military agencies for the sake of national defense and then gradually moves to the public and finally the private sector, at which point they are generally accepted without much opposition(e.g. security check at the airport, security check at libraries, etc,.). Discussing privacy issues, Sherizen said that there are people in Congress who have started asking questions about the use of technology and particularly its duel or neutral nature. He said that they were asking questions about the social and political implications of information systems. He also added that there are many who consider the Privacy Act of 1974 to be clearly outmoded, requiring re-examination to make it more technically effective. Further, he said that MIS managers should question what is to be held private. There is the need to determine and establish who should do what and who is to be in charge, particularly as there is uncertainty as to who owns privacy issues. However, he said that there was no clear line that could help MIS managers decide. Technologically there are problems in controlling privacy and it cannot be done overnight. Also there are very few products and devices available to control privacy.

Discussing the area of security issues, Sherizen said that there is a large market for biometric measures and some of

them (e.g. retinal eye configuration for employee identifying at check-out from work) raise serious questions which have to be resolved. Referring to the security of information within the system, he said that the problem is not only with hackers but more so with authorized users commiting unauthorized acts. Sherizen then briefly discussed the National Security Decision Directive(NSDD) 145 signed in September 1984. This directive he said, has the power to put together and control all information that is thought to affect national security. The organization responsible for this function is to be headed by the NSA. He stated that this directive would have a significant effect on all of us when it is put into practice. Basically, he said that it was a militarization of information.

In closing, Sherizen stated that there is a lot of questioning in Congress at present about the ownership of information. He also referred to the suggestion that there is a way by which we can both have privacy and still use these information systems for our own good. Further, Sherizen anticipated the insurance liability effect having an impact on the privacy issue.

SPEAKERS' COMMENTS AND RESPONSES TO QUESTIONS

The question was raised as to how a DS could be effectively operated without the aid of computer technology such as was done in countries like Russia and France in years gone by. Laudon responding said that totalitarian societies have certainly operated as dossier societies without the aid of advanced technology such as computers. He added that the totalitarian regime is the result of a collapse in the administrative system and not a result of efficient administration. The totalitarian regime does not trust the bureaucratic system and is therefore anti-bureaucratic. Laudon said that though technology cannot be blamed per se for a DS, it could still play a vital role. In effect he said that technology is not neutral but rather a key player and a DS could result if technology is not properly controlled and used.

A member of the audience raised the issue of idealogy and asked how a government that followed a policy of privatization could simultaneously follow a policy of collecting information (making private information public). Sherizen responded saying that the Reagan government is doing something that they would have screamed at if they were in the opposition.

Responding to a question about the commercial use of information, Laudon said that while privacy is not a commodity an individual's name has some value attached to it and people pay for lists of names. However, the individual concerned does not benefit primarily because of market inefficiencies.

Defining the DEFRA Act of 1984, Laudon said that it stood for deficit reduction, and that under it state and federal governments were required to create repositories to hold tax, medical, and social security information. In other words there will be centers in each state that will hold detailed documentation on individuals. Laudon cited this Act as a classic example of transition to a DS taking place gradually and without fanfare.
