

PRIVACY ISSUES

SURROUNDING

PERSONAL IDENTIFICATION

SYSTEMS

James Laban
April, 1996

TABLE OF CONTENTS

INTRODUCTION	3
IDENTITY v IDENTIFICATION	6
THE NEED FOR AN IDENTIFICATION SYSTEM	8
SYSTEM CHOICES	10
HOW FINGERPRINTING WORKS	12
MULTI-PURPOSE IDENTIFICATION SCHEMES	13
CONGRESSIONAL MOVEMENT TOWARD A NATIONAL IDENTIFICATION SYSTEM	15
PRIVACY ISSUES	19
RISKS IN MULTI-PURPOSE IDENTIFICATION SCHEMES	20
THE PUBLIC PERCEPTION OF FINGERPRINTING	21
THE QUESTION OF INTRUSIVENESS	22
<u>DAVIS v MISSISSIPPI</u>	22
<u>THOMAS v NEW YORK STOCK EXCHANGE</u>	23
<u>IACOBUCCI v CITY OF NEWPORT</u>	24
<u>MILLER v MURPHY</u>	24
ISSUES SURROUNDING A NATIONAL ID CARD	25
DISCUSSION	27

In 1995, the Governor's Blue Ribbon Commission on Welfare Fraud made a number of recommendations, including the implementation of a biometric identification system that would deter individuals from attempting to apply for welfare benefits under a fraudulent identity.¹ It was also suggested that a database be established for all General Assistance recipients.

Legislation was subsequently drafted which directed the Commissioners of the Department of Social Services (DSS) and the Department of Motor Vehicles (DMV) to examine the available types of biometric identifier systems, and to the greatest extent possible, select a system that would be compatible with those used in surrounding states.² The legislation required the DSS Commissioner to utilize the system for the General Assistance Program, the AFDC Program, and any other program to be determined at the discretion of the Commissioner. Furthermore, recipients of those programs would be mandated to participate in the system as a condition of program eligibility.

The legislation states that the information obtained from the identification process would be the proprietary information of DSS, and cannot be released or made available to any agency or organization, or used for any purpose other than identification or fraud prevention in this or any other state. One exception is that information may be made available to the office of the chief state's attorney, if necessary, for the prosecution of fraud.

The bill received one of the longest debates of the legislative session.³ Opponents argued that the fingerprinting process was demeaning, in that only criminals are fingerprinted. One such opponent to the bill was State Representative Christopher Donovan, from Meriden. During his remarks on the floor of the House, he pledged that if the Bill was passed, he would have himself fingerprinted in protest.

Despite the opposition, the Bill became law, and effective January 2, 1996, DSS began implementation of the fingerprinting process. For that purpose, DSS contracted with NBS Imaging Systems, Inc., the company currently under contract with the Connecticut DMV for their driver's license digital imaging system. First year operating costs for the DSS program are projected to be \$2.6 million,⁴ but the state expects to save \$7.5 million during that same period. The anticipated savings are based on the assumption that individuals who are presently defrauding the system will not undergo the digital fingerprinting process, and will be dropped from the rolls.⁵ In other words, the state has no expectation of actually identifying and prosecuting welfare cheats ("double dippers"), but only hopes to force them out of the system as a result of the fingerprinting mandate. These expectations are based on the experiences of three other states where similar systems exist. In New York State, 15% of all General Assistance recipients failed to appear for imaging when the program was introduced.⁶ New Jersey's experience was similar (12% failed to appear).⁷ California, where the nation's first program was developed, had 3,021 active recipients refuse to be

fingerprinted when the system was installed, and as a result, were dropped from the public assistance rolls permanently.⁸

Connecticut plans to eventually expand the system to include the Food Stamp and Medicaid programs, and the digital ID cards will be used for electronic benefit transfer.⁹ It also plans to match data with neighboring states, and initial discussions on data exchange took place at the October 11, 1995 meeting of the Northeast Coalition On Fraud Prevention, held in New York City.¹⁰ In addition to DSS fraud prevention purposes, the system might be extended to Connecticut driver's licenses.¹¹ Currently, digital fingerprint imaging is not a prerequisite to obtaining a driver's license.

The system became operational in the Meriden DSS regional office on 2/14/96, and as promised, Rep. Donovan visited the office to stage a mild protest.¹² Accompanied by a few supporters, including his wife and child, Donovan said that the new law was discriminatory, in that it singled out poor people, and that the process carried with it a stigma of criminality. "If you are going to fingerprint poor people, fingerprint us too", Donovan was quoted as saying.¹³ He then seated himself at the operator station, and was digitally imaged.

Many people have voiced concerns over the creation of electronic databases containing personal identification information. Some who may say that it's a good idea to fingerprint welfare recipients, might be reluctant to submit to it themselves as a requirement to obtain a driver's license or passport. The public's concern seems to be focused on the possible uses and misuse of the information captured in these systems.

This paper will address the privacy related public concerns surrounding identification systems in general, with particular emphasis on fingerprinting.

IDENTITY v IDENTIFICATION

Fingerprinting, or digital imaging, is just one type of personal identification system currently available. Before considering the need for such a system, and seeing what is available for system choices, the distinction between "identity" and "identification" should be addressed.

One of the leaders in information technology systems research is Roger Clarke, a former senior information systems academic at the Australian National University (1984-1995). In a recent publication, Clarke differentiates the terms "human identity" & "human identification".¹⁴ He says that "identity" and "identification" are vague and ambiguous terms, and are often treated with considerable looseness by most legal systems, particularly those whose origins can

be traced to Britain.¹⁵

Clarke defines human “identity” as “the condition of being oneself”, noting that since the Renaissance, individuality and human identity have become central to our modern conception of mankind.¹⁶ He says that the integrity of the individual is the central reason for careful expression of human rights in documents like the US Constitution.¹⁷

Human “identification”, on the other hand, is a physical matter, according to Clarke.¹⁸ He says that identification means “the act of establishing the identity of, or recognizing it in information systems. The purpose of identification is to link a stream of data with a person.”¹⁹ Human identification is the “association of data with a particular human being.”²⁰

It’s important to distinguish between these two terms. People who express privacy concerns relating to fingerprinting schemes often claim an invasion of privacy. One of underlying themes of this paper is that the simple process of capturing information relating to a person’s identification, in and of itself, is not an invasion of privacy in most cases. If, however, the information obtained is used improperly, it could lead to the loss of ones’ identity. It is important to keep this distinction of terms in mind while reading the Congressional and judicial responses that follow. Congress, on the one hand, has shown resistance to the notion of a national identification system, and that resistance is perhaps based on the public’s fear of loss of “identity”. The courts seem to take a different view, looking at these schemes as simply being a means of acquiring “identification” information.

THE NEED FOR AN IDENTIFICATION SYSTEM

Most organizations, especially large ones, both public or private, require some type of formal identification system, and an organization’s identification needs grow in proportion to the size of the organization.²¹ When there is growth in an organization, there is, in most instances, a corresponding decrease in trust, and increase in the incident of long-term economic relationships.²² Organizations need reliable identification of the individuals they deal with, whether it be customers served, individuals pursued (law enforcement), or their own employees. In social service agencies, for example, there is a fiduciary need to know to whom income-support is being paid.²³

When deciding what, if any system needs to be developed, the threshold question in many instances is; when is anonymity unacceptable, and identification necessary?²⁴ Once the organization determines that identification is necessary, it has to then consider its specific system needs. These could include: universality of coverage; uniqueness; permanence; indispensability (characteristics that the person retains); collectibility; storability; exclusivity;

precision; simplicity; cost; convenience; or acceptability.²⁵ Additionally, there's a need to achieve an appropriate balance between the harm arising from false-inclusions, and from false-exclusions.²⁶

It is in the self-interest of government agencies and business to establish tighter social control, and a general purpose scheme would be most effective if it was world wide.²⁷ If all people were registered at birth, the scope for people to undertake illegal activities would be greatly constrained.²⁸ Many difficulties in such a scheme would exist, however, including; establishing and maintaining standards; the problems of ensuring a scheme of sufficient integrity; the prevention of forgery; and ongoing quality assurance, to name a few.²⁹ The largest roadblock to a national or worldwide system, however, is public resistance.

SYSTEM CHOICES

There are a variety of means to identify a person; appearance, names, tokens, codes, knowledge, and biometrics.³⁰ The problems associated with using appearance (photo ID's) for identification purposes are apparent. People's looks change; either through the natural process of nature, or through accidental or purposeful alterations, such as cosmetic surgery, hair color change, and the like. A photograph is, therefore, a highly unreliable means of recognizing a person at a later time.³¹

Likewise, there are simply too many uncertainties associated with use of names for identity. Most organizations that use names for identification, require additional elements of identification as confirmation data.³²

Another less desirable method of identifying people is a token based identification system. A token is a thing the person has on his or her possession, such as a marriage certificate, driver's license, or passport, that the individual produces to prove identity.³³ But a driver's license, Social Security card, or birth certificate, however, has little integrity as an identification document.³⁴ It is very easy to obtain false ID's, and a person can easily create one or more false identities. The cost of fraudulent schemes using false ID's is estimated to be \$25 billion annually.³⁵ Thus, token based systems are not effective means of identification.

Codes are somewhat superior to appearance, names, and tokens. It's common for organizations to create coding systems, and in so doing, they can assure the uniqueness of the code.³⁶ Bar coding is one type of coding systems which is widely used.

Another commonly used method is knowledge based identification.³⁷ People may be recognized by demonstrating that they are in possession of information which only that person would be expected to know.³⁸ Many banks and credit card companies will ask for some bit of personal information, such as the applicant's mother's maiden name, which is used as a kind of password to access information on the account.

A biometric identifier is the most reliable solution currently available.³⁹ The term biometric refers to any and all of a variety of identification techniques based on some physical and difficult to alienate characteristic.⁴⁰ They include fingerprints, DNA, voice spectrography, signature dynamics, and hand geometry.⁴¹

Of the available varieties, fingerprinting is the only biometric method of identification currently available that is feasible on a large scale basis. Genetic testing (blood & DNA) is generally viewed as being too intrusive, and the testing process is expensive and slow.⁴² Spectrography and signature dynamics systems are not as desirable because they are less reliable, and more expensive than fingerprinting.

HOW FINGERPRINTING WORKS

Thumbprints and fingerprints have been used since the end of the nineteenth century in matters of a criminal nature.⁴³ In most "free" countries, there is generally no authority for compulsory provision of fingerprints unless one is charged with a crime.⁴⁴ A few countries, including the United States, apply fingerprinting in other areas, such as immigration matters.⁴⁵

Fingerprints were once filed by what was referred to as the Henry Classification, a method somewhat similar to the Dewey decimal system. It grouped the whorls and arches on each print, and counted print ridges. In order to find a match, prints had to be checked manually against those falling in certain classifications. It was a very time consuming process, and it was difficult to locate a match.⁴⁶

The new computer technology has changed all that, and the entire process is done electronically. The fingerprint is scanned into a computer and is digitized. Each minutia, or place at which ridge lines end or split into two, is noted and categorized by its type (end or split), by location, and ridge direction. Four neighboring minutiae are then examined, and the ridges between the minutiae are counted. This process is extended again, and blurred areas of the fingerprint are ignored. Next, relative position and relationship to other ridges is noted and stored on a 512 pixel-per-inch scale. Finally, the relationship of minutiae information obtained is entered into a database. Matching is accomplished as the computer scores how closely a potential match comes to the search print based on the informa-

tion stored in that database.⁴⁷

MULTI-PURPOSE IDENTIFICATION SCHEMES

As stated, there is significant advantage in multiple organizations using a general purpose scheme for identifying individuals with whom they deal. Economies of scale can be gained by combining resources and technologies.⁴⁸ There is worldwide interest in the development of identification schemes, and the technology is rapidly advancing. A common problem found in the United States and other countries, however, is the absence of power to demand proof of identity from citizens. As a result, the integrity of a general-purpose identification scheme is weakened.⁴⁹

The United States, for example, has established the Social Security numbering system, which was initially operated exclusively by the Social Security System for its own purposes. But in 1961, the IRS, for lack of a better system, began using social security numbers for identifying taxpayers.⁵⁰ The integrity of the social security numbering scheme has always been very low, and practically anyone can obtain multiple cards.⁵¹ Despite this weakness, the IRS, and many other U.S. governmental agencies have continued to use social security numbers as the basis for identifying their clients, due to the lack of anything better.⁵²

In contrast, there are governments elsewhere in the world that exert more power over their citizens. In such places, large national identification systems are developing. Motorola recently announced, for example, that it won contracts worth tens of millions of dollars to supply microcontrollers that will form the heart of two new European government health and social security card projects.⁵³ Under the initiatives, Smartcards (credit card size devices incorporating a built-in computer chip) will eventually be issued to the entire Spanish and Czech populations. Spain will issue 40 million social security Smartcards its population, and the Czech republic will run a pilot health insurance Smartcard in the Litomerice region which will involve 10,000 recipients. If successful, they intend to implement a country-wide health card project for 10 million people in 1997 or 1998.

Motorola says that there is a growing trend amongst governments across the world to look at Smartcard solutions for the administration of public-sector services and benefits. "Taken together with the continuing expansion in financial and telecom applications, it's only a matter of time before everyone in Europe carries some form of Smartcard."⁵⁴ They predict a huge expansion in the worldwide demand for Smartcards, and plan to increase pro-

duction of them tenfold by the year 2000 to meet the demand.

Some countries, on the other hand, share a strong tradition of personal freedom and don't have an inhabitant registration system. Examples are the UK, Australia, and New Zealand.⁵⁵

CONGRESSIONAL MOVEMENT TOWARD A NATIONAL IDENTIFICATION SYSTEM

As noted, there is strong resistance in the U.S. toward the notion of a national registry, or unified identification system. In recent years, however, some movement has been apparent at the Congressional level.

In 1976, a U.S. Department of Justice report urged the federal and state agencies to take action against schemes involving fraudulent documents, and urged the private sector to take various remedial actions.⁵⁶ Among them was a recommendation that there be established a national system of matching birth and death records, along with national standards for birth certificates and drivers licenses.⁵⁷

Congress responded by enacting the False Identification Crime Control Act of 1982.⁵⁸ The Act makes it a federal offense to manufacture, traffic in, or illegally possess federal or foreign identification documents.

Then in 1983, the Social Security Amendments of 1983, required the Social Security Administration to design a system for matching death records with social security cards, and to make the social security cards more reliable by using tamper-resistant paper.⁵⁹

Next, the Comprehensive Crime Control Act of 1984, laid the foundation for biometrically supported identification.⁶⁰ The legislative history of the Act notes that its intent was to bring integrity to identification documents, and states that fingerprint impressions provide the only reliable basis for identification. It also mandates the use of common descriptive terms and formats to reduce duplication and redundancy in existing systems. Additionally, it called for a Presidential study to consider comprehensive federal legislation targeted at the identification document problem.

Next, Congress passed the Commercial Motor Vehicle Safety Act of 1986,⁶¹ which created the Commercial Driver's License Identification System (CDLIS). The CDLIS is intended to limit commercial drivers to obtaining just one license. The purpose is public safety, and the system identifies commercial drivers with poor driving records, and makes it a crime for a person to have more than one commercial license. The Act also mandated the creation of a

national commercial driver's license system using state information systems and a federal pointer system, as well as the development of national standards for the issuance and format of the commercial driver's license. This system requires drivers of interstate transports to be finger imaged for licensing purposes.

California became interested in biometric technology, and from 1989 to 1990, the California Motor Vehicle Department conducted the Personal Identifier Project.⁶² The purpose of the demonstration project was to examine the feasibility of two different types of biometric technologies to support the CDLIS. Using finger imaging and retina scan technologies, they tested 62,000 drivers. The results were that finger imaging was 92% accurate, while retina scanning was only 69% accurate.⁶³ California also completed a survey of those participating in the test, and it indicated that there was a high degree of public acceptance of biometrics for identification purposes. 80% of those surveyed found the technology to be "interesting, comfortable, safe, a good idea, easy to use, and important."⁶⁴ Based on the results of this demonstration, California is pursuing a national policy which would mandate all states to tie in to one licensing biometric database.

Congress then passed the Immigration Reform and Control Act of 1986, making it a crime for employers to employ anyone other than a US citizen or an alien with a bona fide work permit.⁶⁵ The Act included several directives aimed at improving identification systems and the integrity of identification documents. Among them was a directive to the Secretary of Health and Human Services to study the feasibility of creating a social security number validation system.

While enacting the Immigration Reform Act, Congress also tried to address growing public concern over the creation of a national identification card system. They added language in the Act which expressly forbids the creation of a national ID card, and mandates that all identification system created under the Act must protect individual privacy. To provide this protection, the Act prohibits the sharing of identification information with criminal justice agencies. Additionally, it expressly states that the identification card does not have to be presented to anyone for any reason other than employment purposes. and adds that it is not necessary to carry the card on one's person.

Congress next passed the Anti-Drug Abuse Act of 1988, containing 20 separate provisions to combat identification fraud.⁶⁶ It mandated that the Attorney General create a reliable system of the identification of felons attempting to buy firearms, and also required positive identification of all pilots, airplane owners, and persons engaging in cash transactions at a federal bank that exceed \$3,000.

Most recently, the Biometric Identification System Act of 1990 (draft legislation) was introduced by Senators Dole and Simpson.⁶⁷ It proposed that a mandatory biometric identification system be instituted by states for driver's licenses, purchasers of firearms, persons crossing the US border, and certain aliens. Under the proposed Act, the Secretary of Transportation would have the responsibility for establishing standards for the system. It sought to create a system in which a person would have one drivers license, one social security number, one passport, and one voter identification card. It sought to ensure that an individual would have but one identity, and that the card would be the person's official form of positive identification. The Act would have given states the responsibility for maintaining the database on its citizens.

The Dole/Simpson legislation wasn't enacted, but a part of it wound up in the proposed Immigration Act of 1990.⁶⁸ The initial draft would have established a pilot program to evaluate the effectiveness of a national biometric driver's license system. Again, language was included to address public concern that such a scheme might become a *de facto* national identification card. It would have prohibited the card being used as a sole means of identification, if other forms of identification could reasonably attest to identity. Additionally, the Act proscribed federal systems in favor of decentralized state-based systems; a further measure of protection against a national card scheme. Lastly, it sought to prevent the linking of identification databases by prohibiting federal agencies from divulging an individual's identification number. The pilot program was deleted, however, from the Immigration Act prior to its enactment on Nov. 29, 1990.⁶⁹

PRIVACY ISSUES

As one can see, Congress has been moving, albeit slowly, toward a national identification system. In the process, there has been consistent public resistance to most governmental and private identification proposals. Accepting this inherent objection to identification, it is necessary to balance the interests of individuals in the various aspects of civil liberties against the collective interest in social control in order to sustain law and order.⁷⁰ Of special concern is the threat to personal privacy rights if general purpose informational databases are created.⁷¹

The need to identify oneself might be distasteful to some; to others an insult to human dignity.⁷² Additionally, there is a great deal of distrust associated with the use of biometric identifiers.⁷³ Fingerprinting continues to be associated with the exercise of power by the state over people, especially in relation to criminal law.⁷⁴ As a result, compulsory fingerprinting has been viewed by many as an invasion of privacy.⁷⁵

RISKS IN MULTI-PURPOSE IDENTIFICATION SCHEMES

The level of public concern becomes much more acute once identification schemes are used for multiple purposes, and public concerns in the US have been well documented.⁷⁶ But at the same time, we have had continual problems with illegal immigration and citizen dishonesty. There have been ongoing proposals by government agencies to upgrade the integrity of the social security numbering system with the intention that it will become an efficient multi-purpose identification scheme, but these proposals have been for the most part unsuccessful, due to public resistance.⁷⁷

In 1969, for example, the American National Standards Institute (ANSI) proposed a standard national identifier. It was decided, however, that the level of distrust in government was such that was not a good idea.⁷⁸

In 1973, and Advisory Committee the US Department of Health, Education & Welfare concluded that a national identifier system should not be established.⁷⁹

The US Privacy Act of 1974 made it unlawful for any agency to deny benefits based solely on the individuals refusal to disclose his SSN.⁸⁰

In order for the government to be successful in implementing an effective identification system, like finger imaging, it needs to identify and address the public policy issues surrounding public resistance toward them. During a government technology conference workshop held in Albany, New York in 1990, three critical public policy issues identified.⁸¹ They were: 1) public perception of fingerprinting , 2) intrusiveness of the process, 3) problems surrounding a national identification system.

1. THE PUBLIC PERCEPTION OF FINGERPRINTING

In the 12th century, fingerprints were used to authenticate documents and to verify identity. It was commonplace, and generally accepted. In the 20th century, however, the public began to associate fingerprinting with criminal arrest. Lately, public perception has begun to change again. Since the use of fingerprinting has been used more and more for employment purposes, licensing, and the like, the public attitude towards it has been more accepting.⁸²

2. THE QUESTION OF INTRUSIVENESS

Does fingerprinting violate one's Constitutional right of privacy?

Courts have consistently upheld federal, state, and local requirements for the submission of fingerprints.⁸³ The

governmental entity must, however, show a compelling governmental interest (rational basis test).⁸⁴

In **Davis v Mississippi**, the Supreme Court found that the fingerprints obtained as a result of an illegal detention were improperly admitted into evidence.⁸⁵ Nevertheless, the court said that “Detention for fingerprinting may constitute a much less serious intrusion upon personal security than other types of police searches and detentions. Fingerprinting involves none of the probing into an individual’s private life and thoughts that marks an interrogation or search.”⁸⁶

In his concurrence, Justice Harlan stated that “There may be circumstances...where compelled submission to fingerprinting would not amount to a violation of the Fourth Amendment, even in the absence of a warrant...”⁸⁷

Justice Stewart went further, claiming that fingerprints should not be looked upon as being evidence in the conventional sense, and said that the fingerprints in this case should have been admissible at trial. “Like the color of a man’s eyes, his height, or his very physiognomy, the tips of his fingers are an inherent and unchanging characteristic of the man.”⁸⁸

In **Thomas v New York Stock Exchange**, the plaintiffs were employees of various stock exchange firms who brought action challenging the constitutionality of a New York statute mandating that all employees of stock exchange firms be fingerprinted as a condition of employment.⁸⁹ The District Court held that the statute did not invade the plaintiff’s right of privacy, nor did it deny them due process.

The plaintiff’s claim in Thomas relied on Davis v Mississippi. The court ruled, however, that said that reliance was misplaced, in that Davis spoke only to improper methods used in obtaining fingerprint evidence in a criminal investigation. The court said that this case was different, in that the fingerprinting was done in a noncriminal context, and the legislation was reasonably related to the purposes sought to be achieved by the regulation. The court, quoting Davis, added, “the slight interference with the person involved in fingerprinting seems to us one which must be borne in the common good.”⁹⁰

The Thomas plaintiffs were also concerned that the fingerprints obtained as a result of the employment procedure might be used for future criminal investigations. The court responded by saying “... even if the plaintiffs were to succeed in establishing that the state intended to incorporate these fingerprints into its central criminal identification files to be used as a means of future crime detection, such a procedure does not run afoul of any constitutional prohibitions ... the state having presented a valid justification under its police power for the original taking of the prints under reasonable circumstances, their use for future identification purposes, even in criminal investigations, is

not impermissible.”⁹¹ The Court added that, “The day is long past when fingerprinting carried with it a stigma of criminality.”⁹² It said that submission of a fingerprint to an employer was no more an invasion of privacy than the submission of a photograph or signature.⁹³

In **Iacobucci v City of Newport**, the plaintiff challenged a city ordinance which required employees of certain liquor establishments to be fingerprinted. The California District Court ruled that taking fingerprints is not a threat to “fundamental human rights” guaranteed by the Constitution, adding that it was reasonable, not arbitrary, and bore a rational relationship to a permissible state objective.⁹⁴

In **Miller v Murphy**, there was a constitutional challenge made to a city regulation requiring pawnbrokers to take fingerprints of their customers.⁹⁵ There, the court held that the city ordinance did not violate the pawnbrokers’ rights to contract or engage in occupation, nor did it violate their customers’ right to privacy. With respect to the customers’ right of privacy, the court said that “... such a slight intrusion is not seen by courts to infringe on interests which must be deemed fundamental.”⁹⁶

3. ISSUES SURROUNDING A NATIONAL ID CARD

Opponents to a national identification system are concerned with the government using the information systems to compile comprehensive dossiers of sensitive information on the lives of citizens.⁹⁷ They believe that the linking of various databases is inevitable, and that the requirement to carry an identification card will follow.

The American Civil Liberties Union, for example, believes that government use of information systems will lead to some form of mandatory national identification card, which, in their opinion, will pose an unjustified threat to individual privacy.⁹⁸ Janiori Goldman, then director of the American Civil Liberties Union’s Privacy and Technology Project, expressed fear that the confidentiality of fingerprint data gathered to fight crime would quickly be breached.⁹⁹ He felt that there would be little to stop immigration authorities, as an example, from retrieving the fingerprints of welfare recipients, or even of credit-card holders, to ferret out illegal aliens.¹⁰⁰ His concern is “cross referencing of fingerprints between the F.B.I., the Department of Motor Vehicles, the Immigration Office, and the welfare office.”¹⁰¹

DISCUSSION

In that the public perception to the criminal stigma attached to fingerprinting is somewhat eroding, and the courts have definitively addressed the privacy issues, it appears that the only real policy issue which still needs to be addressed is the protection and integrity issues surrounding informational databases. The most effective biometric identification system, fingerprinting, can be expected to excite considerable public suspicion, and even hostility.¹⁰² In addition to the public hostility, registration schemes can be important elements in the exercise of control over the majority of people, and deficiencies in any scheme leave room for the seriously dishonest to manipulate it.¹⁰³ Hence the multi-purpose identification schemes can assist in the enforcement of social control over the weak, but do little to influence the powerful, clever and dishonest.¹⁰⁴

Roger Clarke warns that any high-integrity identifier presents a threat to civil liberties, in that it would have enormous power over the populace.¹⁰⁵ “All human behavior would become transparent to the state, and the scope for non-conformism and dissent would be muted.”¹⁰⁶

Another author on the subject, Dianne Zimmerman, warns that the exchange of computerized information poses the greatest threat to privacy today.¹⁰⁷ She suggests that “... privacy law should focus more on identifying and protecting information that warrants it at the points of origin, rather than continuing the practice of imposing liability only after the information is disseminated to the public.”¹⁰⁸ In other words, concern should be focused on the integrity of the informational databases.

George Trubow, Professor of Law and Director of the Center for Informatics Law at the John Marshall Law School, seems to share Zimmerman’s concern about the database integrity. Trubow says we need to have responsible law and policy to ensure that we manage the technology, and not have technology manage us.¹⁰⁹ To the degree the databases house personal information, Trubow has serious privacy concerns, and suggests that we need to develop public policies to deal with database linkages.¹¹⁰ He believes that a single identification number for every individual is needed for the purpose of protecting privacy, but that we need to ensure that identities of people don’t get confused.¹¹¹ If they do, lives can be ruined by misinformation.¹¹² Trubow adds that in his opinion, probably the only valid model for the single identification number is one based on biometrics.¹¹³

In that linkage of databases is likely to flow, Trubow suggests that a federal level, quasi-independent agency be created to monitor the system.¹¹⁴ He says that Congress needs to lift the prohibition of the creation of a national ID, and establish public policy to protect the privacy rights of individuals while serving the legitimate needs of govern-

ment to protect its citizens against fraud.¹¹⁵

Trubow also suggests that a biometric identification scheme, if managed properly, might actually increase an individual's right of privacy, by giving the individual more control over his or her personal information.¹¹⁶ He says that "Personal privacy is not about hiding one's identity, it is about preserving it ... ultimately, privacy is personal integrity."¹¹⁷ Trubow believes that if used effectively, biometric technologies will give people an accurate and reliable form of identification. It will secure a method of identification necessary for personal and business functions, including the electronic transfer of funds, credit card purchases, document authentication, and access to facilities, while at the same time assist the government in combating fraud¹¹⁸

But until such time that the national policies are in place, public concern over identification systems will remain high. Stories relating to misuse of personal information appear in the media almost daily. A recent "60 Minutes" broadcast, for example, chronicled the plight of a New Jersey physician who claimed to have had her "identity" stolen by a group of Nicaraguan criminals.¹¹⁹ The Nicaraguans submitted a fraudulent address change to the Post Office, and had the doctor's mail forwarded to a P.O. Box in New York City. In doing so, they were able to obtain information relating to her bank accounts, social security number, date of birth, and other family information. In a short time they were able to make an extraordinary number of purchases, withdraw funds from her retirement fund, and even transfer money from her children's college savings funds.

The Post Office told the doctor that her situation was not unique, and that these types of criminal operations were commonplace, targeting affluent professionals across the country. The Post Office suggested that there was little she could do to stop them from reselling and reusing her personal information, short of changing her name, and acquiring a new identity. She was dumbstruck in the knowledge that she was being forced to become someone else.

Stories are also commonplace about mistaken identity. A recent story appeared in the Hartford Courant about Luis Colon of Hartford.¹²⁰ Mr. Colon, a long time Hartford resident with solid community ties, was misidentified by a National Crime Information Center computer match, and was arrested on charges that he raped two children in Florida. Granted, Mr. Colon has a very common name, but in this instance, Mr. Colon's Social Security number also matched that of the Florida criminal. Police say that it's still unclear how the Social Security number became linked to the other man, but after a review of file photographs and fingerprints on file, they determined that the Luis Colon of Hartford was not the Luis Colon of Florida.

Even though exonerated, Mr. Colon said that his life has become "absolutely awful." He's quoted as saying "I can't

go out. My professional peers have shunned me. Everywhere I go, people label me as if I'm guilty. People make comments to me in the grocery store.”

The police investigating the mix-up in the system feel confident that they can have erased any record of Colon's arrest, but added that “Colon will pay a greater cost every day of his life. He's going to carry this to his grave.”

Another, more local example of public concern over dissemination of private information, concerns supermarket coupon cards in Connecticut. A recent article reported that certain supermarkets in the state have been capturing information on coupon card holder's buying habits, and then selling that information.¹²¹ One customer, after learning that her purchasing history was being electronically stored, said that she felt she was intentionally misled by the store, and that her privacy had been invaded. In response, legislation has been introduced by Representative Andrew M. Fleischmann, D-West Hartford, to regulate the shopper cards and require full notice of disclosure to the applicant of a card, including an authorization to release information.

Stories like these tend to increase public fear and distrust. At the same time, identification technology continues to evolve, and new uses for it are being discovered every day. It has even been expanded to the identification of animals. A recent Newsweek article reports that a British village of 150 residents is pioneering the use of genetic analysis to identify dog owners who do not clean up after their dogs who “poop” on the streets. Starting soon, owners will be required to submit a few hairs from their animals, from which a DNA genetic profile will be developed. Sidewalk samples will then be matched against the DNA database to identify offenders.¹²²

But, as Don Noel pointed out in a recent editorial, there is no way we can slow down the fast evolving technology in identification systems, and with each new development, more and more private employers and businesses are using them. Commenting on the welfare program fingerprinting mandate, Noel predicted that fingerprinting devices will become so commonplace, that in the very near future ... “their use to deter welfare fraud will be unremarkable.”¹²³

I agree with Noel's prediction, and believe that it is only a matter of time until we are all carrying a card which links us to a national identification database. It is my opinion that now is the time for Congress to address the public policy issues relating to the ongoing expansion of identification systems, in order to assure that individual rights are properly protected. It will be very inefficient and shortsighted to wait until problems surface state to state, and have state legislatures responding with a panoply of stop gap measures. We need a clear national policy, consistent national standards, and centralized regulation of identification systems.

¹ **Connecticut Blue Ribbon Commission on Welfare Fraud, 1995.**

² **Substitute House Bill No. 7010, section 27.**

³ **Don Noel, *With New Technology, There'll be no need to fingerprint Welfare Recipients*, Hartford Courant, Aug. 30, 1995 at A15.**

⁴ **DSS Digital Imaging Fact Sheet, Jan. 1996.**

⁵ **Id., Quoted Source: Office of Policy and Management.**

⁶ **DSS Fact Sheet, *supra* note 4.**

⁷ **DSS Fact Sheet, *supra* note 4.**

⁸ ***Fingerprints Used to Cut Welfare Fraud*, New York Times, Apr. 6, 1992 at A14.**

⁹ **DSS Fact Sheet, *supra* note 4.**

¹⁰ **Id.**

¹¹ **Id.**

¹² ***Welfare Protest Bears Donovan's Fingerprints***, Meriden Record Journal, Feb. 15, 1995 at A1.

¹³ **Id.**

¹⁴ **Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues***, Department of Commerce, Australian National University, 1994.

¹⁵ **Clarke, *supra* note 13.**

¹⁶ **Id.**

¹⁷ **Id.**

¹⁸ **Id.**

¹⁹ **Id.**

²⁰ **Id.**

²¹ **Clarke, *supra* note 13.**

²² **Id.**

²³ **Id.**

²⁴ **Clarke, *supra* note 13.**

²⁵ **Id.**

²⁶ **Id.**

²⁷ **Id.**

²⁸ **Id.**

²⁹ **Id.**

³⁰ **Clarke, *supra* note 13.**

³¹ **Id.**

³² **Id.**

³³ **Id.**

³⁴ **Thomas F. Wilson, *Civil Applications of Automated Fingerprint Identification Systems*, 1 (North American MORPHO Systems, Inc. 1991).**

³⁵ **Id. at 2.**

³⁶ **Clarke, *supra* note 13.**

³⁷ **Id.**

³⁸ **Id.**

³⁹ **Wilson, *supra* note 34 at 3.**

⁴⁰ **Clarke, *supra* note 13.**

⁴¹ **Wilson, *supra* note 34 at 3.**

⁴² **Clarke, *supra* note 13.**

⁴³ **Clarke, *supra* note 13.**

⁴⁴ **Id.**

⁴⁵ **Id.**

⁴⁶ **NEC Technologies Automated Fingerprint Identification System Publication.**

⁴⁷ **NEC Technologies Automated Fingerprint Identification System Publication.**

⁴⁸ **Clarke, *supra* note 13.**

⁴⁹ **Id.**

⁵⁰ **Id.**

⁵¹ **Id.**

⁵² **Clarke, *supra* note 13.**

⁵³ **America Online, London Business Wire, Feb. 13, 1996.**

⁵⁴ **Id.**

⁵⁵ **Clarke, *supra* note 13.**

⁵⁶ **Report on the Federal Advisory Committee on False Identification, *The Criminal Use of False Identification*, U.S. Department of Justice (November 1976).**

⁵⁷ **Wilson, *supra* note 34 at 4.**

⁵⁸ **False Identification Crime Control Act of 1982, Public Law No. 97-398, 18 U.S.C. 1028 (Supp. 1989) and 1738 (1984).**

⁵⁹ **Social Security Amendments of 1983, Public Law No. 98-21, Section 333.**

⁶⁰ **Comprehensive Crime Control Act of 1984, Public Law No. 98-473, 18 U.S.C. 1028 (Supp. 1989).**

⁶¹ **Commercial Vehicle Safety Act of 1986, Public Law No. 99-570.**

⁶² **Wilson, *supra* note 34 at 14.**

⁶³ **Id. at 14.**

⁶⁴ **Id. at 15.**

⁶⁵ **Immigration Reform and Control Act of 1986, Public Law No. 99-603.**

⁶⁶ **Anti-Drug Abuse Act of 1988, Public Law No. 100-690.**

⁶⁷ **Report 101-955, House of Representatives, 101st Congress, 2d Session.**

⁶⁸ **Immigration Act of 1990, Section 522.**

⁶⁹ **Wilson, *supra* note 34 at 9.**

⁷⁰ **Clarke, *supra* note 13.**

⁷¹ **Clarke, *supra* note 13.**

⁷² **Id.**

⁷³ **Id.**

⁷⁴ **Id.**

⁷⁵ **Id.**

⁷⁶ **Id.**

⁷⁷ **Id.**

⁷⁸ **Clarke, *supra* note 13.**

⁷⁹ **Id.**

⁸⁰ **Id.**

⁸¹ **Wilson, *supra* note 34 at 18.**

⁸² **Wilson, *supra* note 34 at 18.**

⁸³ **Id. at 19.**

⁸⁴ **Id. at 19.**

⁸⁵ **Davis v. Mississippi, 394 U.S. 721 (1969).**

⁸⁶ **Id. at 727.**

⁸⁷ **Id. at 728.**

⁸⁸ **Davis, 394 U.S. at 730.**

⁸⁹ **Thomas v. New York Stock Exchange, 306 F.Supp. 1002 (S.D.N.Y. 1969).**

⁹⁰ **Id. at 1010.**

⁹¹ **Thomas, 306 F.Supp. at 1011.**

⁹² **Id. at 1007.**

⁹³ **Id. at 1009.**

⁹⁴ **Iacobucci v. City of Newport, 785 F.2d 1354 (6th Cir. 1986).**

⁹⁵ **Miller v. Murphy, 143 Cal.App.3d 337 (1983).**

⁹⁶ **Id. at 346**

⁹⁷ **Wilson, *supra* note 34 at 19.**

⁹⁸ **Id. at 19. Statement of Wade J. Henderson, Associate Director, Washington Office of the National ACLU, Lucas Guttentag, Director, Immigration Task Force, ACLU, and Janlori Goldman, Staff Attorney, Washington Offices of the National ACLU on Voluntary Work Authorization Cards on H.R. 3374 before the United States House of Representatives, Committee on the Judiciary, Subcommittee on Immigration, Refugees, and International Law, November 9, 1989.**

⁹⁹ **Jacques Steinberg, *Coming Soon: Fingerprints at Many Fingertips*, New York Times, Jan. 10, 1993.**

¹⁰⁰ **Id.**

¹⁰¹ **Id.**

¹⁰² **Clarke, *supra* note 13.**

¹⁰³ **Id.**

¹⁰⁴ **Id.**

¹⁰⁵ **Id.**

¹⁰⁶ **Id.**

¹⁰⁷ Dianne L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 Cornell L. Rev. 291, 362 (1983).

¹⁰⁸ Zimmerman, *supra* note 107 at 362, 363.

¹⁰⁹ Wilson, *supra* note 34 at 20.

¹¹⁰ **Id.**

¹¹¹ **Id.**

¹¹² **Id.**

¹¹³ **Id.**

¹¹⁴ Wilson, *supra* note 34 at 21.

¹¹⁵ **Id.**

¹¹⁶ Wilson, *supra* note 34 at 21.

¹¹⁷ **Id.**

¹¹⁸ **Id.**

¹¹⁹ **60 Minutes**, Feb. 25, 1996.

¹²⁰ **Matthew Kauffman**, *A Nightmare Came To Life In A Common Name*, **Hartford Courant**, Mar. 21, 1996, at A3.

¹²¹ **Anthony Giorgianni**, *Supermarket Coupon Cards Raise Privacy Concern*, **Hartford Courant**, Feb. 21, 1996, at B8.

¹²² *Pets: England's DNA Doggies*, **Newsweek**, Mar. 4, 1996, at 8.

¹²³ **Don Noel**, *With New Technology, There'll be no Need To Fingerprint Welfare Recipients*, **Hartford Courant**, Aug. 30, 1995, at A15.

