The Uniform Driver's License as a National ID

Address by ACLU Associate Director Barry Steinhardt to the American Association of Motor Vehicle Administrators

Feburary 10, 2002
Arlington, Virginia

First, let me thank you for inviting me here this morning to to address the issue of uniform state driver's licenses. It speaks well for your organization's willingness to consider public input and input from diverse viewpoints that you have invited me here to present our views on the AAMVA's proposal.

I. Standardized driver's licenses are a de facto National ID

In the spirit of cooperation that you have displayed, let me emphasize that we have no interest in interfering with the difficult job of making the administration of driver's licenses a smooth and efficient experience. Nor do we want to interfere with your efforts to make the system less prone to error. Commonsense measures do need to be taken to root out fraud in the issuance of licenses. We all want to be safer. We were all affected by the events of September 11.

On September 11 at 8:48 when the first plane in hit the World Trade Center, I was on the runway at LaGuardia airport on a shuttle about take off for Washington, when my plane was stopped dead in its tracks. I watched in horror as smoke billowed up from lower Manhattan, only a few blocks from the ACLU's offices and knowing that full well that my brother-in-law, who I later learned thankfully got out safely, was in the tower that was hit.

September 11 was a day that will be forever seared into my memory.

No matter your proximity to ground zero, we all want to be safe! But simply put, the creation of a uniform national driver's license is a de facto National ID card system, which offers only the illusion of security, while threatening our fundamental liberties.

To the credit of the AAMVA leadership, you have been intellectually honest in acknowledging the far-reaching ramifications of your proposal. Your spokespeople have said in their media statements that there is no need for a federally issued National ID when a uniform driver's license of the sort you propose would serve the same purpose.

Indeed, there are several possible routes by which we could end up with a national ID. Congress could directly enact it. It could evolve out of one of the traveler's ID cards that the airline industry has proposed. But the most likely source for a national ID is the route that the AAMVA has suggested. It is this reality that brings me here today.

II. ID Cards in any form won't prevent terrorism

The rationale for creating a national ID after September 11, no matter what its guise, is to create a clear line between "us" (innocent people) and "them" (dangerous terrorists). Unfortunately, none of the proposed identification systems would effectively sort out the "good" from the "bad." At best, an identification card simply confirms that you are who you say you are. At worst, an ID card will serve as proof of a false identity that will lull us into a false sense of security.

ID cards, whether legitimate or false, do not establish bad motive or intent. All 19 of the September 11 hijackers had social security numbers (SSNs) most legitimate, some not. One of the hijackers was listed in the San Diego phone book - both name and address. And still others rented automobiles with their debit cards and lived as quite law-abiding residents in suburban Florida neighborhoods. The purpose of a "sleeper cell," after all, is to live as quietly and unobtrusively as possible.

A uniform ID card or driver's license would have done nothing to establish their criminal motives for renting cars, going to flight school or boarding those planes.

Nor would it offer certain proof of identity.

First, there is the problem of breeder documents that are used to obtain driver's licenses. After all, an identity card is only as good as the information that establishes a person's identity in the first place. Birth certificates - California actually had theirs on line - and Social Security cards can be forged, bought, or stolen. The Inspector General of the Social Security Administration testified in November that six of the hijackers obtained SSNs through fraudulent means. And, at least one person who is a suspected associate in the September 11 attack has been indicted for using false information to obtain a SSN.

It does not make sense to build a national identification system on a faulty foundation, particularly when possession of an ID card would give a terrorist a free pass to avoid heightened security measures.

Driver's licenses derived from foreign passports may be even more problematic. Some countries don't even use birth certificates; what will stop terrorists from laundering passports and ID documents through these countries, then applying for US driver's licenses (in someone else's name) in this country?

Secondly, a national driver's license ID system - especially one with added smart card features like embedded biometrics - will increase the incentive for dishonest DMV employees to sell fake IDs, which will become all the more valuable. It is not pleasant to

discuss, but insider fraud is real. For instance, in 1990, several DMV employees in Virginia were indicted for selling possibly thousands of drivers' licenses to illegal immigrants in violation of the law. A recent report from a grand jury convened by the Florida Attorney General confirmed the black market in phony driver's licenses exists in that state. Enhancing the value of these documents will only make it more lucrative. The creation of these cards and supporting infrastructures create new risks of insiders issuing phony IDs and outsiders gaining access.

And a super driver's license will not solve the epidemic problem of identity theft, as some have suggested, but rather worsen it.

The driver's license doesn't factor into all that many ID theft cases. Most thieves get along just fine without a driver's license. All they need is your SSN and name, and if they can get it, your Date of Birth. So the majority of ID theft cases will not be thwarted by a national ID system of uniform driver's licenses. Criminals will always be able to come up with false IDs and ways to beat the system.

And ID theft victims may face a new nightmare. What happens if someone gets an ID in your name with his biometrics on it? How does one reestablish one's identity under those circumstances?

III. The Social Consequences of the Uniform Driver's License as National ID.

As Americans, we are, of course, concerned for the safety of our nation. The first test of any proposed security measure is whether it will be effective. The driver's license as National ID fails that test, and there should be no need to even debate the social consequences of the plan. In any commonsense calculus, ineffectiveness should end the debate. But regrettably, it is not likely to here.

So let me now focus on the social consequences of the uniform driver's license as National ID. This idea is dangerous for America as a society: it would facilitate the creation of the surveillance society that Americans have always resisted. And it would produce new forms of discrimination. Let me explain why we believe that is the case.

Privacy has risen to the fore of our national conscience largely because of the confluence of two developments. First, vast increases in computing power now make it possible to collect enormous amounts of data, and search through it for the tiniest detail in seconds. New data mining techniques let database owners sort through and analyze billions and billions of pieces of data. Secondly, distributed networks like the Internet allow lightning-fast communication of personal data, too often for reasons that are unrelated to the purpose for which it was collected.

But the days when most sensitive information was safely deposited in practical obscurity in a clerk's drawer are long over.

And as a result of all these new technologies, there is a kind of pent-up capacity for surveillance. There is a huge amount of data collection and data storage and processing power in American life right now. But all this increasing collection of data is taking place in a not-quite-organized way. Grocery stores, for example, use "loyalty cards" to keep detailed records of what customers buy, using some of that massive computer power that is now so easily available. Amazon keeps records of what we read. The airlines keep track of where we fly. Credit card companies keeps track of what we buy, and where we are when we buy it.

For someone concerned about privacy, none of these trends are good. But what would be much, much worse would be for an organizing principle to come along and provide a way by which all these pools of data that are out there can be organized, linked together, centralized into a single, incredibly rich dossier or profile of our lives.

A colleague of mine with greater knowledge of science reminded me that in chemistry there is something called a saturated solution; for example a glass of water with a large amount of sugar dissolved into it. The sugar molecules will continue to circulate randomly and disconnectedly through the glass of water in liquid form, but if you drop a precipitate into it such as a string, all those sugar molecules will suddenly get organized and line up into a solid crystal. What we're afraid of is that a national ID will act as a precipitate, and all the information gathering that's going on out there randomly and disconnectedly will get organized around the ID and lead to the creation of what amounts to national database of sensitive information about American citizens. And as you know, the data doesn't literally have to reside in the same computer. It could be spread across thousands of separate databases, but if it is indexed the same way in each, and can be searched all at once, then what you have for all practical purposes, is a single database.

So we believe that you will be creating a standard not just for driver's licenses, but for the collection of personal information. And once that standard is in place, it will be the ideal tool for organizing all the new data that is being gathered. How long before office buildings, doctors' offices, gas stations, highway tolls, subways and buses incorporate the ID card into their security or payment systems for greater efficiency? Day to day, individuals will be asked for ID more and more often. Every time a police officer, security guard, or store scans your ID card with a pocket bar-code reader, it will create a permanent record of that check, including the time and location. The result will be a nation where citizens' movements inside their own country are monitored and recorded through these "internal passports."

Of course, supporters of the various national ID proposals always believe that they will be able to offer privacy protections. I believe that the AAMVA is quite genuine in offering these protections as part of your proposal. But history teaches us that even the best-intended safeguards will not remain in place for very long. The most prominent example is the social security number. When my parents and grandparents were issued their numbers as adults, federal law prohibited its use for any purpose other than to administer the brand new social program. My children, who were issued their numbers as infants, know that the government's promise has long since been broken. Function creep

is the primary rule of databases and identifiers. Databases and identifiers that are created for once purpose are almost inevitably used for others.

A distributed national ID system in the form of a standardized driver's license will become a Frankenstein monster that is much, much more than the AAMVA, or the state DMVs, or the driver's license system as a whole can contain. Neither you nor any other groups will be able to control it or limit its functions.

Once the first step is taken in setting up the national ID infrastructure, the pressure for expansion of the system will be intense. Law enforcement and other government agencies will of course link into it. Soon employers will want access too; the American Trucking Association is now apparently lobbying to join airlines in having the authority to check FBI databases so that it can perform checks, not just on drivers but on back-office workers. Soon landlords would demand access, and credit agencies, and mortgage brokers, and private investigators, civil litigants, direct mailers, and so on and so on.

A national ID system would violate the freedom Americans take the most for granted and the one that most defines our liberty: the right to be left alone.

Beyond the very real problem of the inevitably growing number of authorized uses, there will be the problem of unauthorized abuses. Thousands and thousands of government officials would have access to the massive database of personal information required to support a national system of driver's licenses. Even now internal breaches of database information occur on a regular basis at both the federal and state levels. In 1997, the General Accounting Office found serious weaknesses in the IRS's computer security and privacy protections. An investigation by the Detroit Free Press documented how Michigan law enforcement personnel regularly abused their access to the so-called crime computer to help their friends or themselves stalk women, threaten motorists, track estranged spouses - even to intimidate political opponents. In New York City a whistleblower reported that a police video surveillance system was used by male officers for what amounted to sexual voyeurism.

Any one of these privacy violations would be magnified in the context of a national ID system. With data increasingly tied together thanks to the national ID "standard," fraud or error would no longer be limited to one state law enforcement database or set of federal tax files. Government employees could tap into a database that included all kinds of information about an individual - from tax returns to health care data to student loan information. One bad employee or one wrong keyboard stroke could send a person's entire file into public distribution.

Rather than eliminating discrimination, as some have claimed, a national identity card in any form would foster new forms of discrimination and harassment of anyone perceived as looking or sounding "foreign." That is what happened after Congress passed the Employer Sanctions provision of the Immigration Reform and Control Act of 1985: widespread discrimination against foreign-looking American workers, especially Asians and Hispanics. A 1990 General Accounting Office study found almost 20 percent of

employers engaged in discriminatory practices. A super driver's license would have the same effect on a massive scale, as Latinos, Asians, Muslims, and persons of Middle Eastern descent become subject to ceaseless status and identity checks from police, banks, merchants and others. Failure to carry a national ID card would likely come to be viewed as a reason for search, detention or arrest of minorities. The stigma and humiliation of constantly having to prove that they are Americans or legal immigrants would weigh heavily on such groups

What then can DMVs do to fight fraud, short of establishing a de facto national ID system? DMVs can take many low-tech steps to thwart ID theft, without having to resort to establishing a national ID system. They can take greater care in matching photos on file with the person standing at the desk. They can do a SSN match with the Social Security Administration data base, which is being done now in California with great success. They can tighten their procedures in many other ways, which the California DMV has done, based on the recommendations of its Identity Theft Task Force.

To sum up, it is important with any potentially invasive new system to balance the benefits and the risks. The risks to our society presented by a standardized driver's license or other form of national ID would be substantial. And those risks would not be balanced out by a significant and clearly demonstrable benefit in reducing the danger of terrorism or crime.

# # #