independence institute

Issue Backgrounder

13952 Denver West Parkway • Suite 400• Golden, Colorado 80401
www.IndependenceInstitute.org • 303-279-6536

Colorado Needs Comprehensive Protection for Government Compelled Data

IB-2006-B • February 2006
By Mike Krause
Justice Policy Initiative

One by-product of advancing technology is the unprecedented ability to collect, analyze, use and store information generated by the day-to-day lives of people. On one hand, this information gathering ability is highly beneficial, creating new efficiencies in, among other things, medicine, credit-granting, shipping and commerce, and even in government.

The information age also has a downside. Advancing technology often helps along identity theft and fraud, creates new ways to invade individual privacy, and new ways to abuse authority.

Advancing technology often helps along identity theft and fraud, creates new ways to invade individual privacy, and new ways to abuse authority.

Most laws empowering citizens with regard to information collected about them concerns the private sector. For instance as of July 2006, thanks to legislation signed by Governor Bill Owens[1], Coloradoans will have the right to "freeze" their credit reports. This law still allows—with the individuals permission—credit reports to be used for credit-granting purposes, but empowers individuals to deny would be identity thieves the ability to open credit in their names.

But many Coloradoans inherently understand that they have less to fear from the private sector collecting data on them than from the government doing so.

Writer P.J. O'Rourke makes this point, "Wal-Mart, while it may sell guns, it doesn't have guns."[2] In other words, the worst a corporation can do with your data is to try to sell you things. The state, on the other hand, has a legal monopoly on the use of force, and the government's ability to track and monitor the lives of its citizenry might be used to criminalize, or otherwise marginalize, those who live their lives in a way unpopular with whoever happens to hold power.

The state, on the other hand, has a legal monopoly on the use of force, and the government's ability to track and monitor the lives of its citizenry might be used to criminalize, or otherwise marginalize, those who live their lives in a way unpopular with whoever happens to hold power.

In other words if information is power, then information gathered and used by government needs to be regulated.

The obvious answer is less government data collection, but unfortunately state compelled information gathering is only going to increase (more on this later).

The next best thing is comprehensive data privacy legislation that state government has to obey, and which empowers citizens.

The next best thing is comprehensive data privacy legislation that state government has to obey, and which empowers citizens.

There are numerous good reasons for such a law:

Piecemeal Protections often Fall Short

In 2001, the Colorado Legislature allowed the state's Division of Motor Vehicles (DMV) to use biometric technology to map applicants' faces for driver's licenses, allowing access to the DMV database to "aid a federal, state or local government agency in carrying out such agency's official function,"[3] in other words, for any purpose whatsoever. The legislature later refined the face-mapping scheme, requiring "a reasonable suspicion that a crime has been committed or will be committed and a reasonable suspicion that the image requested is either the perpetrator of such a crime or the victim of such a crime."[4]

- A comprehensive data law presupposes that of course there needs to be a good reason to tap such a database.

Misuse of Data

In 2003, it was discovered that some Colorado Sheriffs were entering concealed carry gun permit holders (those Coloradoans who go out of their way to abide by state law) into the Colorado Crime Information Center (CCIC).[5] CCIC is a statewide database that is used by law enforcement to, among other things, identify "people and property involved in crime; members of criminal gangs; stolen property; criminal suspects; criminal methods of operation."[6]

- A comprehensive data law would make such data private, and require notification as to how the data will be used, thus allowing citizens to know if complying with the law will make them criminal suspects.

Outright Abuse

In 2002, the Detroit Free Press uncovered at least 90 instances of criminal misuse, by dispatchers, police officers, and federal agents, of Michigan's Law Enforcement Information System (LEIN), a database that utilizes the FBI's National Crime Information Center, Michigan vehicle registration and driving records, and other databases.

The LEIN abuse included doing favors for friends, stalking women, digging up dirt on an ex-spouse's new husband, tipping off criminal suspects to ongoing investigations and, in one case, identifying owners of cars with bumper stickers supporting a candidate for sheriff, by a deputy of the incumbent sheriff.[7]

The LEIN abuse included doing favors for friends, stalking women, digging up dirt on an ex-spouse's new husband, tipping off criminal suspects to ongoing investigations and, in one case, identifying owners of cars with bumper stickers supporting a candidate for sheriff, by a deputy of the incumbent sheriff.

Despite the fact that it is a misdemeanor crime to misuse the system, of the over three dozen police officers found to have abused the system only three faced criminal prosecution.[8] Vagaries in Michigan law differentiated between "official misuse" and "general misuse". In other words, if a police officer abused the system for personal reasons, or to help a fellow officer, it did not rise to a criminal offense. Only if the information was shared with a civilian did the misdemeanor kick in.

- A comprehensive data law would set clear penalties, even for "official" abuse of data.

Government Data Collection is a Growth Industry

Data collection on Coloradoans as a matter of law is only going to grow, making comprehensive protection all the more important.

1. The federal 'Real ID Act' is scheduled to go into effect in 2008.[9] Real ID federalizes state drivers' license standards and issuance. Among other things, the Act will require the Colorado Division of Motor Vehicles to verify, copy and store electronically all the breeder documents such as the birth certificate and social security card, required to prove such things as your address and citizenship, and makes its databases "interoperable" with other states. The Colorado Division of Motor Vehicles will be fundamentally changed from an agency that administers driver's licenses and vehicle registrations to a centralized national identity registry.

- A data protection law would put clear boundaries on how such a registry can, and cannot, be used.

2. In 2005, the Colorado Legislature created an electronic prescription drug-monitoring program.[10] The names of patients and the types of controlled substances they are prescribed and purchase will be collected in a centralized database searchable by a number of different fields. The prescription drug monitoring database is a huge threat to medical privacy, as with the knowledge of what prescription drugs an individual takes, the medical condition of that individual can easily be extrapolated.

The prescription drug monitoring database is a huge threat to medical privacy, as with the knowledge of what prescription drugs an individual takes, the medical condition of that individual can easily be extrapolated.

The legislature made unauthorized releasing, obtaining or attempting to obtain information from the program a civil offense, with any fines paid being deposited back into the prescription drug monitoring fund. In other words, the legislature has created a hugely intrusive monitoring program that will actually profit from its own misuse.

- A data protection law would allow a private right of action against government employees who misuse such an intrusive database.

Identity Theft/Fraud

According to the *2005 Identity Fraud Survey Report*,[11] jointly released by the Better Business Bureau and Javelin Strategy and Research, the third most common way information is obtained for identity theft and fraud is "Corrupt employee who had access to the info."[12] In addition, the fourth most likely person to misuse your personal information (13 percent of cases) is "Someone at a company w/access to personal information."[13]

The key to identity theft is the Social Security Number (SSN). State government widely collects and uses the SSN for numerous purposes never intended.[14] Some examples include:

1. Colorado Department of Revenue uses the SSN as a taxpayer identification number.

2. Division of Motor Vehicles uses the SSN as a "unique identifier" for driver's license and identification card issuance.

3. The SSN is required to obtain a Colorado hunting or fishing license.

In other words, the information needed to commit identity theft and fraud is readily available at numerous state agencies, and to numerous state employees.

...the information needed to commit identity theft and fraud is readily available at numerous state agencies, and to numerous state employees.

In 2004, a computer hacker accessed more than 1.4 million records containing, among other things, names, addresses, and SSNs, from a University of California at Berkeley computer.[15] The data had been transferred to the University for a research study from the California Department of Health and Human Services.

- A data protection law would clearly define why and when SSNs are collected and used by government, require notification to citizens as to how they will be stored and used, require the stripping of SSNs from research data, criminalize misuse of the SSN, and allow a private right of action for violations against both government agencies and employees.

Third Party Data

In May 2005, the New Jersey Court of appeals ruled that police must obtain a warrant to examine power company records. The case stems from the case of a suspected marijuana grower. New Jersey State Police used a subpoena to obtain the electricity bills of a New Jersey man and some of his neighbors. The records were then used to obtain a search warrant for the man's home. In its ruling, the Court of Appeals bluntly stated, "The warrantless seizure of defendant's electric bills was illegal."

In May 2005, the New Jersey Court of appeals ruled that police must obtain a warrant to examine power company records.

- A data protection law would limit "fishing expeditions" by government using third party data such as utility and banking records.

A Data Law in Action

The state of Minnesota has a comprehensive data protection law, the "Minnesota Data Practices Act."[16]

In 2003, it was discovered that the Minnesota Chiefs of Police Association, (MCPA) a private organization, was operating a database called the Multiple Jurisdiction Network Organization (MJNO).

The MCPA uploaded files from various police agencies, including gun permit and juvenile records, and a variety of police "contact" information.[17] The MCPA then classified the information as confidential "criminal investigative data" and made the database available back to law enforcement agencies throughout the state. MJNO was created with no legislative permission or oversight, and in near secrecy.

A detailed opinion on the legality of MJNO as it pertains to the Minnesota Data Practices Act. Among the findings:

1. MJNO was collecting and sharing information, including gun permit records, which are considered private under Minnesota law and require notification to the applicant as to how it will be used, "There is no authority from the legislature for these data to be transferred to a statewide database like MJNO whether operated by government or a private party".

2. MJNO contained among other things, "arrest, request for service and response or incident data," and according to the analysis, "These are data elements that are always public. In other words they cannot be classified as 'active criminal investigation data.'"

3. The MCPA as a private entity has no authority to classify anything as confidential, "As the MCPA is not a law enforcement agency, it cannot make the determination that data are active criminal investigative data."

MJNO was collecting and sharing information, including gun permit records, which are considered private under Minnesota law and require notification to the applicant as to how it will be used...

It was determined that the MJNO was illegal under the "Data Practices Act", and the program was shut down.

- A data protection law would require legislative permission and oversight of creation and use of databases containing data collected by government.

Elements of a Data Protection Law[18]

What Does a Data Privacy Law do?

- Controls how government data are collected, created, stored, used, and released.
- Applies to state entities and all political subdivisions including counties, cities, school districts, special districts, boards, commissions, and districts and authorities created by state law, local ordinance, or charter provision.
- Applies to persons or entities licensed or funded by, or under contract to, a government entity.

What are government data?

- Government data are any data recorded by any government entity, or as a matter of law.
- Includes data stored on paper, or in electronic form, including audio or video tape.

What a Data Privacy Law Would Regulate

- What information can be collected
- The classification of specific types of government data
- Duties of government personnel in administering provisions of the law
- Minimum security standards for protecting the integrity of data
- Procedures for classifying data as not public
- Civil and criminal penalties for violations of the law

Classifications of Data

Data on Individuals	Meaning of Classification	Data not on Individuals
Public	Available to anyone for any reason	Public*
Private	Available only to the data subject and anyone authorized by the data subject or by law to see it	Nonpublic
Confidential	Not available to the public or the data subject**	Protected Nonpublic

* Includes Private or confidential data which have been stripped of any data that would identify an individual.

** For example: Criminal investigative data

In the Cato Institute paper "Watching You: Systematic Federal Surveillance of Ordinary Americans," Law Professor Paul Swartz notes that "Americans no longer know how their personal information will be applied, who will gain access to it and what decisions will be made with it."[19]

But at the state level, Coloradoans should be able to know these things, and the Colorado Legislature has the ability to make sure that they do.

INDEPENDENCE INSTITUTE is a non-profit, non-partisan Colorado think tank. It is governed by a statewide board of trustees and holds a 501(c)(3) tax exemption from the IRS. Its public policy research focuses on economic growth, education reform, local government effectiveness, and Constitutional rights.

JON CALDARA is President of the Independence Institute.

DAVID B. KOPEL is Research Director at the Independence Institute, and a columnist for the *Rocky Mountain News*.

MIKE KRAUSE directs the Justice Policy Inititative at the Independence Institute.

Endnotes

[1] CRS 12-14.7-101 "Credit Report Security Freeze Act."

[2] O'Rourke, P.J., National Public Radio, Fresh Air, June 10, 2004.

[3] "Governor doesn't want face-recognition technology abused," 7News, TheDenverChannel.com, July 2001. http://www.thedenverchannel.com/news/879856/detail.html

[4] Krause, Mike and Kopel, David, "Face the Facts," *Reason*, October 2002. http://www.reason.com/0210/fe.dk.face.shtml

[5] "At Least One Colorado Sheriff Entering Concealed Carry Permit Holders into Criminal Database," Rocky Mountain Gun Owners, January 20, 2003. http://www.rmgo.org/alerts/2003-ccic.shtml

[6] Colorado Bureau of Investigation, Program Support Unit, Crime Information Center Unit Functions and Objectives. http://cbi.state.co.us/ccic/default.asp

[7] "Cops tap database to harass, intimidate," *Detroit Free Press*, July 31, 2001.

[8] "Penalties uneven for data misuse," *Detroit Free Press*, August 01, 2001.

[9] The Real ID Act is part of the much broader Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. No. 109-13, 119 Stat. 231 (May 11, 2005). http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00418:

[10] CRS 12-22-7

[11] "2005 Identity Fraud Survey Report," Javelin Strategy and Research, January 2005. http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html

[12] The number one way information is obtained, "Lost/stolen wallet, checkbook, or credit card." Number two is "Friends, acquaintances, relatives w/ access to the info."

[13] Three most likely people, according to the survey, are family member/relative, complete stranger, or a friend/neighbor/in-home employee."

[14] The original purpose of the SSN was to administer Social Security contributions and payments, nothing more.

[15] Sullivan, Bob, "California data leak raises questions," MSNBC, October 27, 2004.

[16] Minnesota Revised Statutes, Chapter 13. http://www.revisor.leg.state.mn.us/stats/13/01.html

[17] Howe, Patrick, "Growing use of private police network raises concerns," *Associated Press*, October 30, 2003.

[18] These elements and definitions are taken from the "Minnesota Data Practices Act," Chapter 13 of the Minnesota Revised Statutes.

[19] Twight, Charlotte, "Watching You: Systematic Federal Surveillance of Ordinary Americans," Cato Institute Briefing Paper No. 69, October 17, 2001. http://www.cato.org/pubs/briefs/bp-069es.html