LEGISLATIVE RESEARCH REPORT

NOVEMBER 20, 2008

REPORT NUMBER 09.031

STATE LAWS REGARDING BIOMETRIC PRIVACY

PREPARED FOR SENATOR BILL WIELECHOWSKI

BY ROGER WITHINGTON, LEGISLATIVE ANALYST

You asked for information regarding privacy. Specifically, you wished to know what states, if any, have laws that prohibit the collection of a person's biometric data, such as a fingerprint or deoxyribonucleic acid (DNA), for purposes other than law enforcement.

As you may know, the term "biometrics" is used for the various ways humans can be identified through unique aspects of their bodies. Fingerprints are probably the most commonly known biometric identifier. Other biometric identifiers include hand prints, vein dimensions, iris designs, blood vessels on retinas, body odor, walking characteristics, voice patterns, facial features, and genetic profile.[1]

The National Conference of State Legislatures (NCSL) collects information on actions state legislatures have taken to safeguard a persons' genetic information.[2] One common theme in state law is to protect employees and job seekers from genetic screening and discrimination. In Table 1, we provide NCSL's summary of state employment laws that pertain to a person's genetic information. As you can see from Table 1, genetic nondiscrimination in employment laws is now in place in 35 jurisdictions. In addition, laws in 19 states prohibit an employer from requesting genetic information or a genetic test from an employee; laws in 26 states prohibit an employer from requiring genetic information or a genetic test from an employee; laws in 16 states prohibit an employer from performing a genetic test on an employee; laws in 11 states prohibit an employer from obtaining an employee's genetic information or genetic test result; and laws in 14 states specify penalties for genetic discrimination in employment. As examples, we include as Attachment A genetic nondiscrimination employment laws from Arkansas, Iowa, New Hampshire, Oklahoma, and Wisconsin.

---

[1] The Privacy Rights Clearinghouse, *http://www.privacyrights.org/ar/Privacy-IssuesList.htm.*

[2] NCSL's summary of state genetic privacy laws can be found at *http://www.ncsl.org/programs/health/genetics/prt.htm.* Alaska's Genetic Privacy law can be found at AS 18.13.010 through AS 18.13.100.

907-465-3991
907-465-3908 (fax)

Alaska Legislature
Legislative Research Services
w3.legis.state.ak.us/laa/research/research.php

State Capitol
Juneau, AK 99801

Table 1: State Genetic Privacy in Employment Laws	
Provisions	**State**
Genetic discrimination prohibited in hiring, firing, and/or terms, conditions or privileges of employment	Arizona, Arkansas, California, Connecticut, Delaware, District of Columbia, Hawaii, Idaho, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Oklahoma, Oregon, Rhode Island, South Dakota, Texas, Utah, Vermont, Virginia, Washington, Wisconsin
Employer Prohibited From Requesting Genetic Information Genetic Test	Arkansas, Connecticut, Idaho, Iowa, Kansas, Louisiana, Maryland, Massachusetts, Minnesota, Nevada, New Hampshire, New York, Oklahoma, Oregon, Rhode Island, South Dakota, Utah, Virginia, Wisconsin
Employer Prohibited From Requiring Genetic Information Genetic Test	Arkansas, Connecticut, Hawaii, Idaho, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, Nevada, New Hampshire, New York, Oklahoma, Oregon, Rhode Island, South Dakota, Texas, Utah, Vermont, Virginia, Washington, Wisconsin
Employer Prohibited From Performing Genetic Test	California, Iowa, Louisiana, Massachusetts, Michigan, Minnesota, Nevada, New Hampshire, New York, Oklahoma, Oregon, Rhode Island, South Dakota, Vermont, Virginia, Wisconsin
Employer Prohibited From Obtaining Genetic Information Genetic Test Result	Arkansas, Idaho, Kansas, Massachusetts, Michigan, Minnesota, New York, Oklahoma, Oregon, South Dakota, Utah
Specific Penalties for Genetic Discrimination in Employment	Arkansas, Idaho, Iowa, Minnesota, Missouri, New Hampshire, New Mexico, Oklahoma, Rhode Island, South Dakota, Utah, Vermont, Virginia, Wisconsin
Notes:	Current through November 2007. Arizona Revised Statutes, §41-1463; Arkansas Code Annotated, §11-5-401 to 405; California Code Annotated, Government Code §12926 and §12940; General Statutes of Connecticut, §46a-60; Delaware Code Annotated, §19-710 to 711; District of Columbia Code, §2-1401.01; Hawaii Revised Statutes, § 378-01 to 10; Idaho Code, §39-8301 to §39-8304; Illinois Compiled Statutes, §410-513/25 and §215 ILCS 5/356v; Iowa Code, §729.6; Kansas Statutes Annotated, §44-1002, §44-1009; Louisiana Statutes, §23:302, §23:303; Maine Revised Statutes, 5 §19301 and 5 §19302; Annotated Code of Maryland, Human Relations Commission §49B-15 to 16; Massachusetts General Laws, §151B; Michigan Compiled Laws, §37.1201, §37.1202; Minnesota Statutes, §181.974; Missouri Revised Statutes, §375.1300, §375.1306; Revised Statutes of Nebraska, §48-236; Nevada Revised Statutes, §613.345; New Hampshire Revised Statutes, §141-H; New Jersey Statutes, §10:5-5, §10:5-12; New Mexico Statutes, §24-21-1 to 7; New York Consolidated Laws, Executive Code §292, §296; General Statutes of North Carolina, §95-28.1A; Oklahoma Statutes, §36-3614.2; Oregon Revised Statutes, §659A.300 to 306; General Laws of Rhode Island, §28-6.7-1; South Dakota Compiled Laws, § 60-2-20; Texas Code, Labor Code 2§21-402; Utah Code, §26-45-103; Vermont Statutes, §18-9333; Code of Virginia, §40.1-28.7:1; Revised Code of Washington, §49.44.180; Wisconsin Statutes, §111.372.
Source:	National Conference of State Legislatures, *http://www.ncsl.org/programs/health/genetics/ndiscrim.htm.*

The state laws described above do not generally extend privacy protections to non-genetic based biometric identifiers such as fingerprints. We were unable to locate a comprehensive list of state laws that prohibit the collection of a person's non-genetic biometric data. In conjunction with NCSL, we searched the statutes of each state for laws that pertain, to some degree, to an individual's non-genetic biometric data and identified 33.

Most of the laws identified by our search are quite dissimilar; they range from preventing schools from collecting the biometric information of students without the written consent of the student's parent or guardian, to establishing inmate telephone systems within state prisons that can identify inmates through biometric identifiers. None of these laws, however, appear to pertain to your

issue of expressly prohibiting employers from collecting non-genetic biometric information from their employees or prospective employees.[3] We include each of these 33 laws as Attachment B; a brief summary of each of these laws is as follows.

Arizona Revised Statutes § 15-109: Prevents schools from collecting biometric information from a pupil unless the pupil's parent or guardian gives written permission.

California Codes, Civil Code § 52.7: Except as provided in law, a person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device.

California Codes, Financial Code § 13082: Adding tactually discernible numerical keypad, such as fingerprint biometrics, to point-of-sale devices to aid visually impaired individuals.

California Codes, Penal Code § 637.3: With the exception of peace officers carrying out his or her official duties, no person or entity shall use any system which examines or records in any manner voice prints, or other voice stress patterns of another person to determine the truth or falsity of statements made by such other person without his or her express written consent given in advance of the examination.

California Codes, Penal Code § 4017.1: Except as provided in law, any person confined in a county jail, industrial farm, road camp, or city jail who is required or permitted by an order of the board of supervisors or city council to perform work, and any person while performing community service in lieu of a fine or custody or who is assigned to work furlough, may not be employed to perform any function that provides access to personal information of private individuals, including the following: addresses; telephone numbers; health insurance, taxpayer, school, or employee identification numbers; mothers' maiden names; demand deposit account, debit card, credit card, savings account, or checking account numbers, PINs, or passwords; social security numbers; places of employment; dates of birth; state or government-issued driver's license or identification numbers; alien registration numbers; government passport numbers; unique biometric data, such as fingerprints, facial scan identifiers, voice prints, retina or iris images, or other similar identifiers; unique electronic identification numbers; address or routing codes; and telecommunication identifying information or access devices.

Connecticut General Statutes § 17b-30: Requires the Commissioner of Social Services and the Commissioner of Motor Vehicles to examine available biometric identifier systems to be used by the state's temporary family assistance program and any other program determined by the Commissioner of Social Services.

---

[3] The list does not include laws that states have adopted in relation to the National Crime Prevention and Privacy Compact or laws that refer to biometrics information in specific identity theft laws. The National Crime Prevention and Privacy Compact Act is a federal law that establishes a method by which states can exchange criminal records for noncriminal justice purposes without charging each other for the information. The URL for the Federal Bureau of investigation's National Crime Prevention and Privacy Compact Act website is *http://www.fbi.gov/hq/cjisd/web%20page/cc.htm.*

Florida Annotated Statutes § 311.125: Establishes the Uniform Port Access Credential Card, which is required of those individuals who work at Florida's seaports. This card must include at a minimum a digital full-face photograph, a digital fingerprint, a multilayered security process, a two-dimensional barcode with technology specifications that will allow the unique biometric identifiers to reside in the barcode, a unique identifying code or number, scanning capability to compare required identifiers with information on file in the central database.

Illinois Compiled Statutes 105 ILCS 5/10-20.40 and 105 ILCS 5/34-18.34: Establishes minimum policies for school districts that collect biometric information from students.

Illinois Compiled Statutes 740 ILCS 14/1 (2008), Biometric Information Privacy Act: Relates to the retention, destruction, and privacy of an individual's biometric information. Prohibits unauthorized disclosure and exempts such information from the Freedom of Information Act. Establishes that no provision be construed to conflict with the Criminal Identification Act; the Private Detective, Alarm, Security, Fingerprint Vendor, and Locksmith Act, or another similar act.

Indiana Statutes § 4-1-6-2: Limits the collection, maintenance, and use of personal information, including voice prints, by state agencies, to that which is relevant and necessary to accomplish a statutory purpose.

Indiana Statutes § 26-2-8-116: Allows electronic signature authentication and identification to be used for certain individuals, under certain circumstances.

Louisiana Revised Statutes 37:1182: Grants the Louisiana Board of Pharmacy the authority to require applicants for any pharmacological license, registration, certificate, permit, or any other designation, to provide the information necessary to verify an applicant's identity including birth certificates, passport documents, legal status documents, and any other biometric information deemed appropriate by the board.

Nebraska Revised Statutes § 87-802: Requires that individuals be notified in the event of a security breach that compromises their personal information. Personal information is defined as a name in combination with another identifying data element, including a fingerprint, voice print, or retina or iris image, or other unique physical representation.

Nevada Revised Statutes § 639.2353: Allows a prescription to be transmitted electronically without the health care practitioner's signature if it contains a facsimile signature, security code or other unique identifier; or a voice recognition system, biometric identification technique or other approved security system is used to identify the practitioner.

New Hampshire Revised Statutes 91-A:10: Prevents the state from releasing data sets that contain biometric identifiers.

New Hampshire Revised Statutes 260: 10-b: Prohibits the collection and retention of any biometric data in connection with motor vehicle registration, operation, and driver licensing. "Biometric data" includes voice data used for comparing live speech with a previously-created speech model of a person's voice.

New Jersey Statutes § 39:2A-29: Permits the New Jersey Motor Vehicle Commission to make technological improvements including the modernization of software and hardware, the addition of surveillance cameras, alarms, and access systems, and the use of biometrics.

North Carolina General Statutes § 130A-480: Prohibits the collection of biometric identifiers, including voice prints, within statute that directs the State Health Director to develop a "syndromic" surveillance program for hospital emergency departments in order to detect and investigate public health threats resulting from a terrorist incident or epidemic.

Ohio Revised Code 3701.75: Establishes standards for using electronic signatures in health care records. One standard requires that some electronic signature systems use either a two-level access control mechanism that assigns a unique identifier to each system user or a biometric access control device.

Oregon Revised Statutes § 807.024: Requires a person who applies for issuance, renewal or replacement of a driver license, driver permit or identification card to submit to collection of biometric data by the Department of Transportation for the purpose of establishing his or her identity.

Pennsylvania Statutes § 1802: Appointees, employees and prospective employees engaged in the service of the Commissions or the Board of Gaming shall submit to fingerprinting and photographing by the Pennsylvania State Police or by a local law enforcement agency.

South Carolina Code § 30-2-10: Requires that all state agencies, boards, commissions, institutions, departments, and other state entities develop privacy policies and procedures to ensure that the collection of personal information (including biometric identifiers) pertaining to the citizens of South Carolina is limited to such personal information required by any such entity to fulfill a legitimate public purpose.

Texas Statutes, Business and Commerce Code § 35.50: Provides that biometric identifiers may not be captured for commercial purposes except with prior notification and consent. Additionally provides that once captured, the biometric information may not be sold, leased, or otherwise disclosed unless the individual consents to the disclosure; the disclosure completes a financial transaction that the individual requests or authorizes; the disclosure is required or permitted by a federal or state statute; or the disclosure is made by or to a law enforcement agency for a law enforcement purpose.

Texas Statutes, Business and Commerce Code § 503.001: Defines a "biometric identifier" as a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry. This law establishes that a person may not capture a biometric identifier of an individual for commercial purposes unless the person informs the individual before capturing the biometric identifier, and receives the individual's consent to capture the biometric identifier.

Texas Statutes, Government Code § 495.025: The State requests proposals from private vendors for a contract to provide pay telephone service to eligible inmates confined in facilities operated by the department. The telephone system must have the capacity to use a biometric identifier of the inmate making the call.

Texas Statutes, Government Code § 531.1063: The Texas Health and Human Services Commission and the Texas Department of Human Services shall develop and implement a Medicaid Fraud Pilot Program. The program must include participant smart cards and biometric readers that reside at the point of contact with Medicaid providers, recipients, participating pharmacies, hospitals, and appropriate third-party participants; and a secure finger-imaging system that is compliant with the Health Insurance Portability and Accountability Act (HIPAA).

Texas Statutes, Government Code § 560.001: Provides that a government body in possession of a biometric identifier may not sell, lease, or otherwise disclose the information unless the individual consents to the disclosure; the disclosure completes a financial transaction that the individual requests or authorizes; the disclosure is required or permitted by a federal or state statute; or the disclosure is made by or to a law enforcement agency for a law enforcement purpose.

Texas Statutes, Transportation Code § 521.032: Establishes the Enhanced Driver's License or Personal Identification Certificate which requires the applicant to submit a biometric identifier as designated by the Department of Transportation.

Vermont Statutes 23 V.S.A. § 634: Prevents the Department of Motor Vehicles from implementing any procedures or processes for identifying applicants for licenses, learner permits, or non-driver identification cards that involve the use of biometric identifiers.

Virginia Code § 2.2-3801 through § 2.2-3809: Includes voice prints in the definition of personal information. Requires that state agencies collect, maintain, use, and disseminate only that personal information permitted or required by law. This law prohibits agencies from disseminating information to another system without specifying requirements for security and usage including access limitations, and receiving reasonable assurances that those requirements and limitations will be observed.

Revised Code of Washington § 46.20.037: This law requires implementation of a voluntary biometric matching system for driver's licenses and identification cards within two years of the full implementation of the Real ID Act. This law states that the biometric matching system is to be used only to verify the identity of an applicant for a renewal or duplicate driver's license or identification card by matching a biometric identifier submitted by the applicant against the biometric identifier submitted when the license was last issued.

West Virginia Code § 17B-2-12a: Vision screening conducted as part of driver's licensure shall not be used to collect any type of personal biometric identifying information.

Included in your request was a document entitled "The Alaskan Biometric Collection Act." As you may know, within this document the author notes that the University of Alaska, Fairbanks requires individuals taking the Certified Public Accountant (CPA) examination to submit to fingerprinting before and possibly during the examination. This fingerprint condition is, however, required by the American Institute of Certified Public Accountants (AICPA), the national, professional organization for all Certified Public Accountants which sets the auditing standards and the ethical standards for all CPAs; the National Association of State Boards of Accountancy (NASBA), which

serves as a forum for the boards of accountancy throughout the United States; and Prometric, which provides testing services for those seeking to take the CPA exam.[4] According to Ken Bishop, Senior Vice President for NASBA, no state prevents Prometric—or any of its subcontractors (the UAF is one of these subcontractors)—from obtaining fingerprint data from those taking the CPA exam.[5]

I hope you find this information to be useful. Please do not hesitate to contact us if you have questions or need additional information.

[4] The URL for the American Institute of Certified Public Accountants is *http://www.aicpa.org/*. The URL for the National Association of State Boards of Accountancy is *http://www.nasba.org*. The URL for Prometric is *http://www.prometric.com/*.

[5] Ken Bishop, Senior Vice President for NASBA, can be contacted at 615-312-3755. In addition, Mr. Bishop notes that Prometric doesn't capture or retain a copy of an individual's fingerprint. Prometric captures an algorithm, or a mathematical representation, based on a person's fingerprint.

Attachment A

Arkansas Code Annotated, §11-5-401 to 405; Iowa Code, §729.6; New Hampshire Revised Statutes, §141-H; Oklahoma Statutes, §36-3614.2; Wisconsin Statutes, §111.372

Attachment B

Arizona Revised Statutes § 15-109; California Codes, Civil Code § 52.7; California Codes, Financial Code § 13082; California Codes, Penal Code § 637.3; California Codes, Penal Code § 4017.1; Connecticut General Statutes § 17b-30; Florida Annotated Statutes § 311.125; Illinois Compiled Statutes 105 ILCS 5/10-20.40 and 105 ILCS 5/34-18.34; Illinois Compiled Statutes 740 ILCS 14/1 (2008), Biometric Information Privacy Act; Indiana Statutes § 4-1-6-2; Indiana Statutes § 26-2-8-116; Louisiana Revised Statutes 37:1182; Nebraska Revised Statutes § 87-802; Nevada Revised Statutes § 639.2353; New Hampshire Revised Statutes 91-A:10; New Hampshire Revised Statutes 260: 10-b; New Jersey Statutes § 39:2A-29; North Carolina General Statutes § 130A-480; Ohio Revised Code 3701.75; Oregon Revised Statutes § 807.024; Pennsylvania Statutes § 1802; South Carolina Code § 30-2-10; Texas Statutes, Business and Commerce Code § 35.50; Texas Statutes, Business and Commerce Code § 503.001; Texas Statutes, Government Code § 495.025; Texas Statutes, Government Code § 531.1063; Texas Statutes, Government Code § 560.001; Texas Statutes, Transportation Code § 521.032; Vermont Statutes 23 V.S.A. § 634; Virginia Code § 2.2-3801 through § 2.2-3809; Revised Code of Washington § 46.20.037; West Virginia Code § 17B-2-12a

Attachment A

Arkansas Code Annotated, §11-5-401 to 405; Iowa Code, §729.6; New Hampshire Revised Statutes, §141-H; Oklahoma Statutes, §36-3614.2; Wisconsin Statutes, §111.372

11-5-401. Title.

This subchapter shall be known and may be cited as the "Genetic Information in the Workplace Act".

History. Acts 2001, No. 1407, § 1.

11-5-402. Definitions.

As used in this subchapter, unless the context otherwise requires:

(1) "DNA" means deoxyribonucleic acid;

(2) "Employer" means employer as the term is defined in Section 3(d) of the Fair Labor Standards Act of 1938;

(3) (A) "Genetic information" means information derived from the results of a genetic test.

(B) "Genetic information" shall not include:

(i) Family history;

(ii) Results of a routine physical examination or test;

(iii) Results of a chemical, blood, or urine analysis;

(iv) Results of a test to determine drug use;

(v) Results of a test for the presence of the human immunodeficiency virus; or

(vi) Results of any other test commonly accepted in clinical practice at the time it is ordered by the insurer;

(4) (A) "Genetic test" means a laboratory test of the DNA, RNA, or chromosomes of an individual for the purpose of identifying the presence or absence of inherited alterations in the DNA, RNA, or chromosomes that cause a predisposition for a clinically recognized disease or disorder.

(B) "Genetic test" shall not include:

(i) A routine physical examination or a routine test performed as a part of a physical examination;

729.6 Genetic testing.

1. As used in this section, unless the context otherwise requires:

a. "Employer" means the state of Iowa, or any political subdivision, board, commission, department, institution, or school district, and every other person employing employees within the state.

b. "Employment agency" means a person, including the state, who regularly undertakes to procure employees or opportunities for employment for any other person.

c. "Genetic testing" means a test of a person's genes, gene products, or chromosomes, for abnormalities or deficiencies, including carrier status, that are linked to physical or mental disorders or impairments, or that indicate a susceptibility to illness, disease, impairment, or other disorders, whether physical or mental, or that demonstrate genetic or chromosomal damage due to environmental factors.

d. "Labor organization" means any organization which exists for the purpose in whole or in part of collective bargaining, or dealing with employers concerning grievances, terms, or conditions of employment, or of other mutual aid or protection in connection with employment.

e. "Licensing agency" means a board, commission, committee, council, department, examining board, or officer, except a judicial officer, in the state, or in a city, county, township, or local government, authorized to grant, deny, renew, revoke, suspend, annul, withdraw, or amend a license or certificate of registration.

f. "Unfair genetic testing" means any test or testing procedure that violates this section.

2. An employer, employment agency, labor organization, licensing agency, or its employees, agents, or members shall not directly or indirectly do any of the following:

a. Solicit, require, or administer a genetic test to a person as a condition of employment, preemployment application, labor organization membership, or licensure.

b. Affect the terms, conditions, or privileges of employment, preemployment application, labor organization membership, or licensure, or terminate the employment, labor organization membership, or licensure of any person who obtains a genetic test.

3. Except as provided in subsection 7, a person shall not sell to or interpret for an employer, employment agency, labor organization, or licensing agency, or its employees, agents, or members, a genetic test of an employee, labor organization member, or licensee, or of a prospective employee, member, or licensee.

4. An agreement between a person and an employer, prospective employer, employment agency, labor organization, or licensing agency, or its employees, agents, or members offering the person employment, labor organization membership, licensure, or any pay or benefit in return for taking a genetic test is prohibited.

5. An employee, labor organization member, or licensee, or prospective employee, member, or licensee who acted in good faith shall not be discharged, disciplined, or discriminated against in any manner for filing a complaint or testifying in any proceeding or action involving violations of this section. An employee, labor organization member, or licensee, or prospective employee, member, or licensee discharged, disciplined, or otherwise discriminated against in violation of this section shall be compensated by the employer, employment agency, labor organization, or licensing agency in the amount of any loss of wages and benefits arising out of the discrimination.

6. This section may be enforced through a civil action.

a. A person who violates this section or who aids in the violation of this section is liable to an aggrieved

Last update: Wed Aug 16 21:03:56 CDT 2000
URL: /IACODE/1999SUPPLEMENT/729/6.html
jhf

TITLE X
PUBLIC HEALTH

CHAPTER 141-H
GENETIC TESTING

Section 141-H:1

141-H:1 Definitions. – In this chapter:

I. "Disability income insurance" means insurance intended to protect against loss of occupational earning capacity arising from injury, sickness, or disablement, including insurance that provides benefits for overhead expenses or purchase of a business or profession when the insured becomes disabled.

II. "Employment" means work performed by an employee for an employer for remuneration.

III. "Employment agency" has the meaning given in RSA 354-A:2, VIII.

IV. "Genetic testing" means a test, examination, or analysis which is generally accepted in the scientific and medical communities for the purpose of identifying the presence, absence, or alteration of any gene or chromosome, and any report, interpretation, or evaluation of such a test, examination, or analysis, but excludes any otherwise lawful test, examination, or analysis that is undertaken for the purpose of determining whether an individual meets reasonable functional standards for a specific job or task.

V. "Health insurance" means any arrangement with any entity which pays medical claims on behalf of an individual, an employee, or dependents, including any such arrangement evidenced by a hospital or medical policy or certificate, hospital or medical service plan or contract, or health maintenance organization group or individual subscriber contract, or self insurance plan or contract, or other evidence of coverage, except for the purposes of this chapter, "health insurance" shall not mean life, disability income, or long-term care insurance.

VI. "Individual" means a human being.

VII. "Labor organization" has the meaning given in RSA 354-A:2, X.

VIII. "Licensing agency" means a unit of government which is authorized to grant, deny, renew, revoke, suspend, annul, withdraw, or amend an occupation license.

IX. "Life insurance" means insurance in which the risk contemplated is the death of a particular individual upon which event the insurer pays a stipulated sum, or the type of insurance defined in RSA 401:1, III.

X. "Long-term care insurance" means the types of insurance defined in RSA 415-D:3, V.

XI. "Person" includes a human being, an association or organization, a trust, corporation, and partnership.

Source. 1995, 101:1, eff. Jan. 1, 1996.

Section 141-H:2

141-H:2 Conditions of Genetic Testing. –

I. Except as otherwise provided in this chapter, no individual or member of the individual's family shall be required to undergo genetic testing as a condition of doing business with another person.

II. Except as required to establish paternity under RSA 522, or as required to test newborns for metabolic disorders under RSA 132:10-a, or as required for purposes of criminal investigations and prosecutions, or as is necessary to the functions of the office of chief medical examiner, no genetic testing shall be done in this state on any individual or anywhere on any resident of this state based on bodily materials obtained within this state, without the prior written and informed consent of the individual to be tested, the parent, guardian, or custodian if the individual is a minor under the age of 18, or the legal guardian or conservator if the individual is an incompetent person. The results of any such test shall be provided only to those persons approved in writing by the individual, the parent, guardian, or custodian if the individual is a minor under the age of 18, or the legal guardian or conservator if the individual is an incompetent person. No person shall refuse to perform genetic testing, or to arrange for genetic testing to be performed, or to do business with an individual, solely because the individual to be tested refuses to consent to providing the test results to some

Source. 1995, 101:1, eff. Jan. 1, 1996.

Section 141-H:5

141-H:5 Use of Genetic Testing in Life, Disability Income, and Long-term Care Insurance. –

I. Except as provided in paragraph II of this section, the provisions of this chapter shall not apply to the provision of life insurance, disability income insurance, or long-term care insurance.

II. A person in the business of providing life, disability income, or long-term care insurance who obtains information with respect to any genetic testing of an individual or a member of the individual's family shall not use that information in writing a type of insurance coverage other than life, disability income, or long-term care insurance.

Source. 1995, 101:1, eff. Jan. 1, 1996.

Section 141-H:6

141-H:6 Civil Action. – An aggrieved individual may bring a civil action under this chapter and, if successful, shall be awarded special or general damages of not less than $1,000 for each violation, and costs and reasonable legal fees.

Source. 1995, 101:1, eff. Jan. 1, 1996.

§36-3614.2.

§36-3614.2.

A. This section shall be known and may be cited as the "Genetic Nondiscrimination in Employment Act".

B. For purposes of the Genetic Nondiscrimination in Employment Act:

1. "DNA" means deoxyribonucleic acid;

2. "Employer" means employer as such term is defined in Section 3(d) of the Fair Labor Standards Act of 1938, 29 U.S.C., Section 203(d);

3. "Genetic information" means information derived from the results of a genetic test. Genetic information shall not include family history, the results of a routine physical examination or test, the results of a chemical, blood or urine analysis, the results of a test to determine drug use, the results of a test for the presence of the human immunodeficiency virus, or the results of any other test commonly accepted in clinical practice at the time it is ordered by the insurer;

4. "Genetic test" means a laboratory test of the DNA, RNA, or chromosomes of an individual for the purpose of identifying the presence or absence of inherited alterations in the DNA, RNA, or chromosomes that cause a predisposition for a clinically recognized disease or disorder. "Genetic test" shall not include:

a. a routine physical examination or a routine test performed as a part of a physical examination,

b. a chemical, blood, or urine analysis,

c. a test to determine drug use,

d. a test for the presence of the human immunodeficiency virus, or

e. any other test commonly accepted in clinical practice at the time it is ordered by the insurer; and

5. "RNA" means ribonucleic acid.

C. For purposes of distinguishing between or discriminating against or restricting any right or benefit otherwise due or available to an employee or prospective employee, other than in connection with the determination of insurance coverage or benefits, no employer shall:

1. Seek to obtain, or use a genetic test or genetic information of the employee or the prospective employee; or

2. Require a genetic test of or require genetic information from the employee or prospective employee.

111.372

111.372 Use of genetic testing in employment situations.

111.372(1)

(1) No employer, labor organization, employment agency or licensing agency may directly or indirectly:

111.372(1)(a)

(a) Solicit, require or administer a genetic test to any person as a condition of employment, labor organization membership or licensure.

111.372(1)(b)

(b) Affect the terms, conditions or privileges of employment, labor organization membership or licensure or terminate the employment, labor organization membership or licensure of any person who obtains a genetic test.

111.372(2)

(2) Except as provided in sub. (4), no person may sell to or interpret for an employer, labor organization, employment agency or licensing agency a genetic test of an employee, labor organization member or licensee or of a prospective employee, labor organization member or licensee.

111.372(3)

(3) Any agreement between an employer, labor organization, employment agency or licensing agency and another person offering employment, labor organization membership, licensure or any pay or benefit to that person in return for taking a genetic test is prohibited.

111.372(4)

(4) This section does not prohibit the genetic testing of an employee who requests a genetic test and who provides written and informed consent to taking a genetic test for any of the following purposes:

111.372(4)(a)

(a) Investigating a worker's compensation claim under ch. 102.

111.372(4)(b)

(b) Determining the employee's susceptibility or level of exposure to potentially toxic chemicals or potentially toxic substances in the workplace, if the employer does not terminate the employee, or take any other action that adversely affects any term, condition or privilege of the employee's employment, as a result of the genetic test.

111.372 - ANNOT.

History: *1991 a. 117.*

Attachment B

Arizona Revised Statutes § 15-109; California Codes, Civil Code § 52.7; California Codes, Financial Code § 13082; California Codes, Penal Code § 637.3; California Codes, Penal Code § 4017.1; Connecticut General Statutes § 17b-30; Florida Annotated Statutes § 311.125; Illinois Compiled Statutes 105 ILCS 5/10-20.40 and 105 ILCS 5/34-18.34; Illinois Compiled Statutes 740 ILCS 14/1 (2008), Biometric Information Privacy Act; Indiana Statutes § 4-1-6-2; Indiana Statutes § 26-2-8-116; Louisiana Revised Statutes 37:1182; Nebraska Revised Statutes § 87-802; Nevada Revised Statutes § 639.2353; New Hampshire Revised Statutes 91-A:10; New Hampshire Revised Statutes 260: 10-b; New Jersey Statutes § 39:2A-29; North Carolina General Statutes § 130A-480; Ohio Revised Code 3701.75; Oregon Revised Statutes § 807.024; Pennsylvania Statutes § 1802; South Carolina Code § 30-2-10; Texas Statutes, Business and Commerce Code § 35.50; Texas Statutes, Business and Commerce Code § 503.001; Texas Statutes, Government Code § 495.025; Texas Statutes, Government Code § 531.1063; Texas Statutes, Government Code § 560.001; Texas Statutes, Transportation Code § 521.032; Vermont Statutes 23 V.S.A. § 634; Virginia Code § 2.2-3801 through § 2.2-3809; Revised Code of Washington § 46.20.037; West Virginia Code § 17B-2-12a

6 of 168 DOCUMENTS

ARIZONA REVISED STATUTES

CURRENT THROUGH THE SECOND REGULAR SESSION OF THE 48TH LEGISLATURE (2008)
Annotations current through cases posted on Lexis.com as of August 10, 2008

TITLE 15. EDUCATION
CHAPTER 1. GENERAL PROVISIONS
ARTICLE 1. GENERAL PROVISIONS

Go to the Arizona Code Archive Directory

A.R.S. § 15-109 (2008)

§ 15-109. Biometric information; prohibition; definition

A. A school in a school district or a charter school shall not collect biometric information from a pupil unless the pupil's parent or guardian gives written permission to collect biometric information from the pupil.

B. At least thirty days before a school in a school district or charter school will collect biometric information, the school shall provide written notice to the parents and guardians of pupils of the intent to collect biometric information. The notice shall include a statement in eighteen point bold-faced capital letters that the parent or guardian must give written permission to collect biometric information from the pupil before the school may collect biometric information.

C. For the purposes of this section, "collect biometric information" means the noninvasive electronic measurement and evaluation of any physical characteristics that are attributable to a single person, including fingerprint characteristics, eye characteristics, hand characteristics, vocal characteristics, facial characteristics and any other physical characteristics used for the purpose of electronically identifying that person with a high degree of certainty.

HISTORY: Laws 2008, Ch. 189, § 1.

NOTES:
EDITOR'S NOTE.
Enacted as § 15-107 and renumbered by the reviser.

11 of 168 DOCUMENTS

*** THIS DOCUMENT REFLECTS ALL URGENCY LEGISLATION ENACTED ***
THROUGH 2007-2008 THIRD EXTRAORDINARY SESSION CH. 7 AND CH. 763 OF THE 2008 REGULAR SESSION APPROVED 9/30/08, AND PROPOSITION 99 APPROVED BY VOTERS 6/3/08

CIVIL CODE
Division 1. Persons
Part 2. Personal Rights

GO TO CALIFORNIA CODES ARCHIVE DIRECTORY

Cal Civ Code § 52.7 (2008)

§ 52.7. Subcutaneous implanting of an identification device; Penalties and remedies; Time for commencing action; Restitution

(a) Except as provided in subdivision (g), a person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device.

(b)

(1) Any person who violates subdivision (a) may be assessed an initial civil penalty of no more than ten thousand dollars ($10,000), and no more than one thousand dollars ($1,000) for each day the violation continues until the deficiency is corrected. That civil penalty may be assessed and recovered in a civil action brought in any court of competent jurisdiction. The court may also grant a prevailing plaintiff reasonable attorney's fees and litigation costs, including, but not limited to, expert witness fees and expenses as part of the costs.

(2) A person who is implanted with a subcutaneous identification device in violation of subdivision (a) may bring a civil action for actual damages, compensatory damages, punitive damages, injunctive relief, any combination of those, or any other appropriate relief.

(3) Additionally, punitive damages may also be awarded upon proof of the defendant's malice, oppression, fraud, or duress in requiring, coercing, or compelling the plaintiff to undergo the subcutaneous implanting of an identification device.

(c)

(1) An action brought pursuant to this section shall be commenced within three years of the date upon which the identification device was implanted.

(2) If the victim was a dependent adult or minor when the implantation occurred, actions brought pursuant to this section shall be commenced within three years after the date the plaintiff, or his or her guardian or parent, discovered or reasonably should have discovered the implant, or within eight years after the plaintiff attains the age of majority, whichever date occurs later.

(L) Photograph.

(M) Fingerprint or other biometric identifier.

(N) Social security number.

(O) Any unique personal identifier.

(4) "Require, coerce, or compel" includes physical violence, threat, intimidation, retaliation, the conditioning of any private or public benefit or care on consent to implantation, including employment, promotion, or other employment benefit, or by any means that causes a reasonable person of ordinary susceptibilities to acquiesce to implantation when he or she otherwise would not.

(5) "Subcutaneous" means existing, performed, or introduced under or on the skin.

HISTORY:

Added Stats 2007 ch 538 § 1 (SB 362), effective January 1, 2008.

Added Stats 2007 ch 538 § 1 (SB 362), effective January 1, 2008.

NOTES:

Hierarchy Notes:

Civ Code Note

Div. 1 Note

Div. 1, Pt. 2 Note

LexisNexis 50 State Surveys, Legislation & Regulations

Civil Rights

12 of 168 DOCUMENTS

*** THIS DOCUMENT REFLECTS ALL URGENCY LEGISLATION ENACTED ***
THROUGH 2007-2008 THIRD EXTRAORDINARY SESSION CH. 7 AND CH. 763 OF THE 2008 REGULAR SESSION APPROVED 9/30/08, AND PROPOSITION 99 APPROVED BY VOTERS 6/3/08

FINANCIAL CODE
Division 4.5. Automated Teller Machine Surcharge Disclosure

GO TO CALIFORNIA CODES ARCHIVE DIRECTORY

Cal Fin Code § 13082 (2007)

§ 13082. Adding tactually discernible numerical keypad to point-of-sale devices to aid visually impaired persons

(a) Whenever a point-of-sale system is changed or modified to include a video touch screen or any other nontactile keypad, the point-of-sale device that would include the video touch screen or nontactile keypad shall also be equipped with either of the following:

(1) A tactually discernible numerical keypad similar to a telephone keypad containing a raised dot with a dot base diameter between 1.5 millimeters and 1.6 millimeters and a height between 0.6 millimeters and 0.9 millimeters on the number 5 key that enables a visually impaired person to enter his or her own personal identification number or any other personal information necessary to process the transaction in a manner that provides the opportunity for the same degree of privacy input and output available to all individuals.

(2) Other technology, such as a radio frequency identification device, fingerprint biometrics, or some other mechanism that enables a visually impaired person to access the video touch screen device with his or her personal identifier and to process his or her transaction in a manner that provides the opportunity for the same degree of privacy input and output available to all individuals.

(b)

(1) On or before January 1, 2010, any existing point-of-sale system, except as provided in paragraph (2), that includes a video touch screen or any other nontactile keypad shall also be equipped with a tactually discernable keypad or other technology as described in subdivision (a).

(2) At locations equipped with two or less point-of-sale machines, only one point-of-sale machine shall be required to be equipped with a tactually discernible keypad or other technology on or before January 1, 2010, as described in subdivision (a).

(c) On and after January 1, 2006, a manufacturer or distributor shall be required to offer for availability touch screen or other nontactile point-of-sale devices to be used and sold in this state that are equipped with tactually discernible keypads or other technology as described in subdivision (a) that enable a visually impaired person to enter his or her own personal identification number or any other personal information necessary to process a transaction in a manner that ensures personal privacy of the information being entered.

1 of 1 DOCUMENT

*** THIS DOCUMENT REFLECTS ALL URGENCY LEGISLATION ENACTED ***
THROUGH 2007-2008 THIRD EXTRAORDINARY SESSION CH. 7 AND CH. 763 OF THE 2008 REGULAR SESSION APPROVED 9/30/08, AND PROPOSITION 99 APPROVED BY VOTERS 6/3/08

PENAL CODE
Part 1. Of Crimes and Punishments
Title 15. Miscellaneous Crimes
Chapter 1.5. Invasion of Privacy

GO TO CALIFORNIA CODES ARCHIVE DIRECTORY

Cal Pen Code § 637.3 (2008)

§ 637.3. Voice stress analyzers

(a) No person or entity in this state shall use any system which examines or records in any manner voice prints or other voice stress patterns of another person to determine the truth or falsity of statements made by such other person without his or her express written consent given in advance of the examination or recordation.

(b) This section shall not apply to any peace officer, as defined in Section 830, while he is carrying out his official duties.

(c) Any person who has been injured by a violator of this section may bring an action against the violator for his actual damages or one thousand dollars ($1,000), whichever is greater.

HISTORY:

Added Stats 1978 ch 1251 § 1.

NOTES:

Collateral References:

Cal Forms Pl & Practice (Matthew Bender) ch 429 "Privacy".

5 Witkin Summary (10th ed) Torts § 660.

Cal Jur 3d (Rev) Assault and Other Wilful Torts § 120; Criminal Law § 1991.

Cal Criminal Defense Prac., ch 20, "Principles of Search & Seizure".

Cal. Legal Forms, (Matthew Bender) § 1C.21[7].

14 of 168 DOCUMENTS

*** THIS DOCUMENT REFLECTS ALL URGENCY LEGISLATION ENACTED ***
THROUGH 2007-2008 THIRD EXTRAORDINARY SESSION CH. 7 AND CH. 763 OF THE 2008 REGULAR SESSION APPROVED 9/30/08, AND PROPOSITION 99 APPROVED BY VOTERS 6/3/08

PENAL CODE
Part 3. Of Imprisonment and the Death Penalty
Title 4. County Jails, Farms and Camps
Chapter 1. County Jails

GO TO CALIFORNIA CODES ARCHIVE DIRECTORY

Cal Pen Code § 4017.1 (2008)

§ 4017.1. Access of specified offenders to personal information

(a)

(1) Except as provided in paragraph (2), any person confined in a county jail, industrial farm, road camp, or city jail who is required or permitted by an order of the board of supervisors or city council to perform work, and any person while performing community service in lieu of a fine or custody or who is assigned to work furlough, may not be employed to perform any function that provides access to personal information of private individuals, including, but not limited to, the following: addresses; telephone numbers; health insurance, taxpayer, school, or employee identification numbers; mothers' maiden names; demand deposit account, debit card, credit card, savings account, or checking account numbers, PINs, or passwords; social security numbers; places of employment; dates of birth; state- or government-issued driver's license or identification numbers; alien registration numbers; government passport numbers; unique biometric data, such as fingerprints, facial scan identifiers, voice prints, retina or iris images, or other similar identifiers; unique electronic identification numbers; address or routing codes; and telecommunication identifying information or access devices.

(2) Notwithstanding paragraph (1), persons assigned to work furlough programs may be permitted to work in situations that allow them to retain or look at a driver's license or credit card for no longer than the period of time needed to complete an immediate transaction. However, no person assigned to work furlough shall be placed in any position that may require the deposit of a credit card or driver's license as insurance or surety.

(b) Any person confined in a county jail, industrial farm, road camp, or city jail who has access to any personal information shall disclose that he or she is confined before taking any personal information from anyone.

(c) This section shall not apply to inmates in employment programs or public service facilities where incidental contact with personal information may occur.

HISTORY:

Hierarchy Notes:

Pt. 3, Tit. 4 Note

Pt. 3, Tit. 4, Ch. 1 Note

LexisNexis 50 State Surveys, Legislation & Regulations

Boot Camps and Prison Farms

23 of 168 DOCUMENTS

LEXISNEXIS (TM) CONNECTICUT ANNOTATED STATUTES

*** THIS DOCUMENT IS CURRENT THROUGH THE 2008 SUPPLEMENT ***
*** ANNOTATIONS CURRENT THROUGH APRIL 16, 2008 ***

TITLE 17b SOCIAL SERVICES
CHAPTER 319o DEPARTMENT OF SOCIAL SERVICES
PART I GENERAL PROVISIONS

GO TO CONNECTICUT STATUTES ARCHIVE DIRECTORY

Conn. Gen. Stat. § 17b-30 (2008)

§ 17b-30. Biometric identifier system.

(a) For purposes of this section, "biometric identifier system" means a system which allows for the recognition of an individual through retinal scanning, finger-imaging, hand geometry or facial recognition. The Commissioner of Social Services and the Commissioner of Motor Vehicles shall examine available biometric identifier systems and to the greatest extent possible, select a system which is compatible with the systems of surrounding states. The Commissioner of Social Services may enter into a memorandum of understanding with the Commissioner of Motor Vehicles for the Department of Motor Vehicles to provide the hardware, software, equipment maintenance, technical training and other resources deemed necessary by the commissioner to establish said system.

(b) At the conclusion or cancellation of the contract entered into pursuant to the memorandum of understanding in subsection (a) of this section, the Commissioner of Social Services may extend the contract for not more than one year, provided, no later than one year after such conclusion or cancellation, the commissioner shall issue a request for proposals for providing the hardware, software, equipment maintenance, technical training and other resources deemed necessary by the commissioner to maintain or improve said system. The subsequent contract for providing the resources for said system shall be awarded pursuant to *section 4a-59* and shall begin no later than one year after such conclusion or cancellation.

(c) Said system shall be utilized for office use only in the following programs: (1) Temporary family assistance; and (2) any other program to be determined at the discretion of the Commissioner of Social Services.

(d) A recipient of a program utilizing said system pursuant to subsection (b) of this section shall participate in said system or be subject to disqualification from such program. The commissioner shall have the authority to exempt a recipient from participation in said system.

(e) The implementation of said system shall begin on or before January 1, 1996. The schedule of such implementation shall be determined by the Commissioner of Social Services.

(f) Biometric identifier information obtained pursuant to subsection (d) of this section shall be the proprietary information of the Department of Social Services and shall not be released or made available to any agency or organization and shall not be used for any purpose other than identification or fraud prevention in this or any other state, except that such information may be made available to the office of the Chief State's Attorney if necessary for the prosecution of fraud discovered pursuant to the biometric identifier system established in subsection (a) of this section or in accordance with *section 17b-90*. The penalty for a violation of this subsection shall be up to a five-thousand-dollar fine or five years' imprisonment or both and the cost of prosecution.

30 of 168 DOCUMENTS

*** Statutes and Constitution are Current through Chapters 2008-2 ***
*** through 2008-6, 2008-208 through 2008-226, 2008-228 through ***
*** 2008-238, 2008-241 through 2008-245, 2008-247, 2008-248 ***
*** 2008-251 through 2008-256 ***
*** Annotations current through May 8, 2008 ***

TITLE 22. PORTS AND HARBORS (Chs. 308-315)
CHAPTER 311. FLORIDA SEAPORT TRANSPORTATION AND ECONOMIC DEVELOPMENT

GO TO FLORIDA STATUTES ARCHIVE DIRECTORY

Fla. Stat. § 311.125 (2008)

§ 311.125. Uniform Port Access Credential System

(1) By July 1, 2004, each seaport identified in *s. 311.09* and subject to the statewide minimum seaport security standards set forth in *s. 311.12* shall be required to use a Uniform Port Access Credential Card that is to be utilized in the operation of the state Uniform Port Access Credential System as required herein. All Uniform Port Access Credential Cards shall be issued by the Department of Highway Safety and Motor Vehicles to the designated port authority, or recognized governing board, of the requesting seaport for distribution to the credential applicant.

(2) (a) The Department of Highway Safety and Motor Vehicles, in consultation with the Department of Law Enforcement, the Florida Seaport Transportation and Economic Development Council, the Florida Trucking Association, and the United States Transportation Security Administration shall develop a Uniform Port Access Credential System for use in onsite verification of access authority for all persons on a seaport as defined in *s. 311.12(2)*, utilizing the Uniform Port Access Credential Card as authorized herein. Each seaport, in a manner consistent with the "Port Security Standards Compliance Plan" delivered to the Speaker of the House of Representatives and the President of the Senate on December 11, 2000, pursuant to *s. 311.12*, and this section, is responsible for granting, restricting, or modifying access authority provided to each Uniform Port Access Credential Card holder and promptly communicating the levels of access or changes in the level of access to the department for its use in administering the Uniform Port Access Credential System. Each seaport is responsible for the proper operation and maintenance of the Uniform Port Access Credential Card reader and access verification utilizing the Uniform Port Access Credential System at its location. The Uniform Port Access Credential Card reader and Uniform Port Access Credential System shall be utilized by each seaport to ensure compliance with the access restrictions provided by *s. 311.12*.

(b) The system shall be designed to conform, as closely as possible, with criteria established by the United States Transportation Security Administration for a Transportation Worker Identification Card, or similar identification, as required by federal law. The system shall, at a minimum, consist of:

1. A centralized, secure database for collecting and maintaining fingerprints and other biometric means of identity, and other information pertaining to personal identification of persons working on, or doing business at, a Florida seaport as set forth in *s. 311.12*;

(8) Each person working on a seaport, as regulated in *s. 311.12(2)*, shall be issued a Uniform Port Access Credential Card upon completion of the application process. Upon issuance of the Uniform Port Access Credential Card, the cardholder is eligible to enter a seaport in the system based on the level of permission allowed by each respective seaport. A person working in a restricted access area must meet the requirements of *s. 311.12(3)*. The Uniform Port Access Credential Card shall be clearly marked for visual verification of the cardholder's permission for access to a restricted area, pursuant to subsection (3). The card must contain biometric verification of the cardholder's identity and proper access permissions. Entrance to a restricted access area, as defined in *s. 311.12(2)*, shall require a machine check and fingerprint verification of each person's Uniform Port Access Credential Card for proper identification. Exit from any restricted access area of a seaport shall require a machine check of the credential card.

(9) Each person not producing a Uniform Port Access Credential Card upon arrival at a restricted area of a seaport must, at a minimum, stop at a check point, show valid identification, and receive a visitor's pass in order to proceed. The visitor's pass must be plainly displayed on the person of the visitor or in the windshield of the vehicle and designate what area of the seaport may be accessed by the visitor. Failure to display the visitor's pass shall result in revocation of a worker's permission to work on the seaport. Public conveyances such as buses carrying passengers into restricted access areas must be able to verify that all passengers have legitimate business on the seaport. Procedures for implementation of this process are the responsibility of each seaport.

(10) The price of a Uniform Port Access Credential Card shall be set by the department and shall reflect the cost of the required criminal history checks, including the cost of the initial state and federal fingerprint check and the annual criminal history check and the cost of production and issuance of the card by the department. A seaport may charge an additional administrative fee to cover the costs of issuing credentials to its employees and persons doing business at the seaport.

(11) Each Uniform Port Access Credential Card remains the property of the State of Florida. Any person possessing such a card shall provide it to any law enforcement officer upon request. A law enforcement officer having reasonable suspicion to believe that a card is possessed or is being used in violation of law or the standards provided by this section, or in any other manner that raises a concern about the safety and security of a seaport, may seize the card. A cardholder has no cause of action against any law enforcement officer who seizes a Uniform Port Access Credential Card.

(12) Each seaport defined in *s. 311.09* and required to meet the minimum security standards set forth in *s. 311.12* shall comply with technology improvement requirements for the activation of the Uniform Port Access Credential System no later than July 1, 2004. Equipment and technology requirements for the system shall be specified by the department no later than July 1, 2003. The system shall be implemented at the earliest possible time that all seaports have active technology in place, but no later than July 1, 2004.

(13) The "Port Security Standards Compliance Plan" delivered to the Speaker of the House of Representatives and the President of the Senate on December 11, 2000, pursuant to *s. 311.12*, shall be updated by the Department of Law Enforcement to reflect the changes made by this act.

(14) This section shall be contingent on the receipt of the federal grant funds necessary to implement the Uniform Port Access Credential System.

HISTORY: s. 2, ch. 2003-96; s. 33, ch. 2005-2.

NOTES:

AMENDMENTS

42 of 168 DOCUMENTS

*** STATUTES CURRENT THROUGH PUBLIC ACT 95-1000 ***
*** ANNOTATIONS CURRENT TO STATE CASES THROUGH SEPTEMBER 12, 2008 ***

CHAPTER 105. SCHOOLS
COMMON SCHOOLS
SCHOOL CODE
ARTICLE 10. SCHOOL BOARDS

GO TO THE ILLINOIS STATUTES ARCHIVE DIRECTORY

105 ILCS 5/10-20.40 (2008)

THIS SECTION HAS MORE THAN ONE DOCUMENT WITH VARYING EFFECTIVE DATES.

§ 105 ILCS 5/10-20.40. Student biometric information

Sec. 10-20.40. Student biometric information. (a) For the purposes of this Section, "biometric information" means any information that is collected through an identification process for individuals based on their unique behavioral or physiological characteristics, including fingerprint, hand geometry, voice, or facial recognition or iris or retinal scans.

(b) School districts that collect biometric information from students shall adopt policies that require, at a minimum, all of the following:

(1) Written permission from the individual who has legal custody of the student, as defined in Section 10-20.12b of this Code[*105 ILCS 5/10-20.12b*], or from the student if he or she has reached the age of 18.

(2) The discontinuation of use of a student's biometric information under either of the following conditions:

(A) upon the student's graduation or withdrawal from the school district; or

(B) upon receipt in writing of a request for discontinuation by the individual having legal custody of the student or by the student if he or she has reached the age of 18.

(3) The destruction of all of a student's biometric information within 30 days after the use of the biometric information is discontinued in accordance with item (2) of this subsection (b).

(4) The use of biometric information solely for identification or fraud prevention.

(5) A prohibition on the sale, lease, or other disclosure of biometric information to another person or entity, unless:

(A) the individual who has legal custody of the student or the student, if he or she has reached the age of 18, consents to the disclosure; or

43 of 168 DOCUMENTS

*** STATUTES CURRENT THROUGH PUBLIC ACT 95-1000 ***
*** ANNOTATIONS CURRENT TO STATE CASES THROUGH SEPTEMBER 12, 2008 ***

CHAPTER 105. SCHOOLS
COMMON SCHOOLS
SCHOOL CODE
ARTICLE 34. CITIES OF OVER 500,000 INHABITANTS -- BOARD OF EDUCATION

GO TO THE ILLINOIS STATUTES ARCHIVE DIRECTORY

105 ILCS 5/34-18.34 (2008)

§ 105 ILCS 5/34-18.34. Student biometric information

Sec. 34-18.34. Student biometric information. (a) For the purposes of this Section, "biometric information" means any information that is collected through an identification process for individuals based on their unique behavioral or physiological characteristics, including fingerprint, hand geometry, voice, or facial recognition or iris or retinal scans.

(b) If the school district collects biometric information from students, the district shall adopt a policy that requires, at a minimum, all of the following:

(1) Written permission from the individual who has legal custody of the student, as defined in Section 10-20.12b of this Code, or from the student if he or she has reached the age of 18.

(2) The discontinuation of use of a student's biometric information under either of the following conditions:

(A) upon the student's graduation or withdrawal from the school district; or

(B) upon receipt in writing of a request for discontinuation by the individual having legal custody of the student or by the student if he or she has reached the age of 18.

(3) The destruction of all of a student's biometric information within 30 days after the biometric information is discontinued in accordance with item (2) of this subsection (b).

(4) The use of biometric information solely for identification or fraud prevention.

(5) A prohibition on the sale, lease, or other disclosure of biometric information to another person or entity, unless:

(A) the individual who has legal custody of the student or the student, if he or she has reached the age of 18, consents to the disclosure; or

(B) the disclosure is required by court order.

*** STATUTES CURRENT THROUGH PUBLIC ACT 95-1000 ***
*** ANNOTATIONS CURRENT TO STATE CASES THROUGH SEPTEMBER 12, 2008 ***

CHAPTER 740. CIVIL LIABILITIES
BIOMETRIC INFORMATION PRIVACY ACT

GO TO THE ILLINOIS STATUTES ARCHIVE DIRECTORY

740 ILCS 14/1 (2008)

§ 740 ILCS 14/1. Short title

Sec. 1. Short title. This Act may be cited as the Biometric Information Privacy Act.

HISTORY: Source: P.A. 95-994, § 1.

NOTES:
EFFECTIVE DATE.
Section 99 of P.A. 95-994 made this Act effective upon becoming law. The Act was approved October 3, 2008.

740 ILCS 14/5 (2008)

§ 740 ILCS 14/5. Legislative findings; intent

Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

HISTORY: Source: P.A. 95-994, § 5.

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

HISTORY: Source: P.A. 95-994, § 15.

740 ILCS 14/20 (2008)

§ 740 ILCS 14/20. Right of action

Sec. 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $ 1,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $ 5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

HISTORY: Source: P.A. 95-994, § 20.

740 ILCS 14/25 (2008)

§ 740 ILCS 14/25. Construction

Sec. 25. Construction. (a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.

(11) 2 members appointed by the chairperson of the Committee, representing the interests of public hospitals; and

(12) 4 public members appointed by the chairperson of the Committee, representing the interests of the civil liberties community, the electronic privacy community, and government employees.

(c) This Section is repealed January 1, 2009.

HISTORY: Source: P.A. 95-994, § 30.

740 ILCS 14/99 (2008)

§ 740 ILCS 14/99. Effective date

Sec. 99. Effective date. This Act takes effect upon becoming law.

HISTORY: Source: P.A. 95-994, § 99.

NOTES:
NOTE.
The Act was approved October 3, 2008.

1 of 1 DOCUMENT

*** Statutes current through the 2008 Second Regular Session ***
*** Annotations current through July 18, 2008 ***

Title 4 State Offices and Administration
Article 1 State Affairs and Offices -- General
Chapter 6 Fair Information Practices

Go to the Indiana Code Archive Directory

Burns Ind. Code Ann. § 4-1-6-2 (2008)

4-1-6-2. Collection of personal information by state agencies -- Records required -- Exchange of information between agencies.

Any state agency maintaining a personal information system shall:

(a) Collect, maintain, and use only that personal information as is relevant and necessary to accomplish a statutory purpose of the agency;

(b) Collect information to the greatest extent practicable from the data subject directly when the information may result in adverse determinations about an individual's rights, benefits and privileges under federal or state programs;

(c) Collect no personal information concerning in any way the political or religious beliefs, affiliations and activities of an individual unless expressly authorized by law or by a rule promulgated by the oversight committee on public records pursuant to IC 4-22-2;

(d) Assure that personal information maintained or disseminated from the system is, to the maximum extent possible, accurate, complete, timely, and relevant to the needs of the state agency;

(e) Inform any individual requested to disclose personal information whether that disclosure is mandatory or voluntary, by what statutory authority it is solicited, what uses the agency will make of it, what penalties and specific consequences for the individual, which are known to the agency, are likely to result from nondisclosure, whether the information will be treated as a matter of public record or as confidential information, and what rules of confidentiality will govern the information;

(f) Insofar as possible segregate information of a confidential nature from that which is a matter of public record; and, pursuant to statutory authority, establish confidentiality requirements and appropriate access controls for all categories of personal information contained in the system;

(g) Maintain a list of all persons or organizations having regular access to personal information which is not a matter of public record in the information system;

(h) Maintain a complete and accurate record of every access to personal information in a system which is not a matter of public record by any person or organization not having regular access authority;

210 IAC 1-6, Title 210. Department of Correction, Article 1. General Provisions, Rule 6. Collection, Maintenance, Release of Offender Records.

405 IAC 1-1, Title 405. Office of the Secretary of Family and Social Services, Article 1. Medicaid Providers and Services, Rule 1. General Provisions.

470 IAC 1-3, Title 470. Division of Family and Children, Article 1. General Administrative Rules, Rule 3. Personnel.

470 IAC 2-1, Title 470. Division of Family and Children, Article 2. Public Assistance, Rule 1. General Public Assistance.

470 IAC 2-5, Title 470. Division of Family and Children, Article 2. Public Assistance, Rule 5. Child Support.

470 IAC 6-1, Title 470. Division of Family and Children, Article 6. Food Stamp Program, Rule 1. Personal Information System.

610 IAC 4-3, Title 610. Department of Labor, Article 4. Safety Education and Training --Occupational Safety, Rule 3. Inspections, Safety Orders and Penalties.

LexisNexis 50 State Surveys, Legislation & Regulations

Commercial Use of Public Records

57 of 168 DOCUMENTS

*** Statutes current through the 2008 Second Regular Session ***
*** Annotations current through July 18, 2008 ***

Title 26 Commercial Law
Article 2 Commercial Transactions
Chapter 8 Uniform Electronic Transactions Act
Part 1. Nongovernmental Electronic Records and Signatures

Go to the Indiana Code Archive Directory

Burns Ind. Code Ann. § 26-2-8-116 (2008)

26-2-8-116. Electronic signature authentication and identification may be used for certain individuals -- Federal and state law not superseded or preempted.

(a) As used in this section, "authorization" means a consent, an approval, or an authorization between an individual and a person.

(b) As used in this section, "electronic identification" means the electronic identification system for form, location, and endorsement that is specified in subsection (d).

(c) Electronic signature authentication and identification may be used for an individual who participates in agreements, authorizations, contracts, records, or transactions that involve individually identifiable health information, including medical records and record keeping, transfer of medical records, medical billing, health care proxies, health care directives, consent to medical treatment, medical research, and organ and tissue donation or procurement.

(d) The electronic authentication and identification under subsection (c) may be accomplished by an interactive system of security procedures that include any of the following:

(1) A tamper proof electric appliance that receives input of unique identification numbers, unique biometric identifiers, or location devices.

(2) A computerized authentication process for biometric identifiers that is linked to the appropriate identification numbers upon receipt of the identifiers.

(3) Transmission of verification of the identifiers to a securely maintained electronic repository.

No provision in this section may be construed to supersede or preempt applicable federal and state law, including the Indiana Uniform Electronic Transactions Act (IC 26-2-8), the Health Insurance Portability and Accountability Act of 1996 and associated regulations, and 21 CFR Part 11.

HISTORY: P.L.77-2005, § 1.

65 of 168 DOCUMENTS

THIS DOCUMENT IS CURRENT THRU THE 2008 1ST & 2ND EXTRAORDINARY SESSIONS
Annotations current through July 8, 2008

LOUISIANA REVISED STATUTES
TITLE 37. PROFESSIONS AND OCCUPATIONS
CHAPTER 14. LOUISIANA PHARMACY PRACTICE ACT
PART 2. BOARD OF PHARMACY

GO TO LOUISIANA STATUTES ARCHIVE DIRECTORY

La. R.S. 37:1182 (2008)

§ 37:1182. Powers and duties of the board

A. The board shall be responsible for the control and regulation of the practice of pharmacy and shall:

(1) Make necessary rules and regulations to carry out the purposes and enforce the provisions of this Chapter and furnish copies of them upon request.

(2) Hold meetings at least once a year and at other times when necessary for the transaction of business that may legally come before it.

(3) Make a written report annually to the governor.

(4) Report to the attorney general of the state all persons violating the provisions of this Chapter.

(5) License by examination applicants who are qualified to engage in the practice of pharmacy under the provisions of this Chapter.

(6) License by reciprocity pursuant to the provisions of this Chapter.

(7) Administer examinations as deemed necessary.

(8) Issue and renew licenses, permits, certifications, registrations, and any other designations deemed necessary to engage in the practice of pharmacy.

(9) Establish and enforce compliance with professional standards and rules of conduct of pharmacists engaged in the practice of pharmacy.

(10) Determine and issue standards for recognition and approval of degree programs of schools and colleges of pharmacy whose graduates shall be eligible for licensure in this state, and the specification and enforcement of requirements for practical training, including internship.

(2) Receive and expend funds, in addition to its annual or biennial appropriation, from parties other than the state, provided that the following conditions are met:

(a) Such funds are awarded for the pursuit of a specific objective which the board is authorized to accomplish by this Chapter, or which the board is qualified to accomplish by reason of its jurisdiction or professional expertise.

(b) Such funds are expended for the pursuit of the objective for which they are awarded.

(c) Activities connected with or occasioned by the expenditures of such funds do not interfere with the performance of the board's duties and responsibilities, and do not conflict with the exercise of the board's powers as specified by this Chapter.

(d) Such funds are kept in a separate, special account.

(e) Periodic reports are made concerning the board's receipt and expenditure of such funds.

(3) Conduct any investigation, inquiry, or hearing which the board is authorized to hold as required by this Chapter.

(4) Place under seal all drugs or devices that are owned by or in the possession, custody, or control of a licensee at the time his license is suspended or revoked or at the time the board refuses to renew his license. Except as otherwise provided in this Section, drugs or devices so sealed shall not be disposed of until appeal rights under the Administrative Procedure Act have expired, or an appeal filed pursuant to that Act has been determined.

(5) Collect professional demographic data.

(6) Employ or contract for inspectors, chemists, agents, clerical help, legal assistance, and other personnel necessary for the proper operation of the board office and for any other purpose under this Chapter.

(7) Establish minimum standards for maintaining the integrity and confidentiality of prescription information and other patient health care information.

(8) Acquire, develop, maintain, expand, sell, lease, mortgage, borrow funds, or otherwise contract with respect to immovable property as it may deem necessary or appropriate to accomplish the provisions of this Chapter. The board shall have the authority to borrow funds with the approval of the State Bond Commission and to expend funds of the board for the acquisition of immovable property and improvements thereon. In the event that the board sells immovable property and improvements thereon, the revenue derived from the sale shall be retained by the board and shall not be subject to reversion to the state general fund.

HISTORY: Acts 1999, No. 767, § 1; Acts 2003, No. 1052, § 2; Acts 2004, No. 131, § 1, eff. Aug. 15, 2004.

NOTES:
LexisNexis (R) Notes:

Amendment Notes

2004 Amendments.

79 of 168 DOCUMENTS

NEBRASKA REVISED STATUTES ANNOTATED

*** CURRENT THROUGH THE 2008 SECOND SESSION AND THE MAY 2008 PRIMARY ELECTION ***
*** ANNOTATIONS CURRENT THROUGH AUGUST 5, 2008 ***

CHAPTER 87. TRADE PRACTICES
ARTICLE 8. FINANCIAL DATA PROTECTION AND CONSUMER NOTIFICATION OF DATA SECURITY BREACH ACT OF 2006

Go to the Nebraska Code Archive Directory

R.R.S. Neb. § 87-802 (2008)

§ 87-802. Terms, defined

For purposes of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006:

(1) Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system;

(2) Commercial entity includes a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal entity, whether for profit or not for profit;

(3) Encrypted means converted by use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key;

(4) Notice means:

(a) Written notice;

(b) Telephonic notice;

(c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in *15 U.S.C. 7001,* as such section existed on January 1, 2006;

(d) Substitute notice, if the individual or commercial entity required to provide notice demonstrates that the cost of providing notice will exceed seventy-five thousand dollars, that the affected class of Nebraska residents to be notified exceeds one hundred thousand residents, or that the individual or commercial entity does not have sufficient contact information to provide notice. Substitute notice under this subdivision requires all of the following:

NOTES:
OPERATIVE DATE:
July 14, 2006.

USER NOTE: For more generally applicable notes, see notes under the first section of this heading.

LexisNexis 50 State Surveys, Legislation & Regulations

Non-Customer Personal Data Security, Breach & Notification

82 of 168 DOCUMENTS

*** This document is current through the 74th (2007) Session and 24th Special (2008) Session ***
*** ANNOTATIONS CURRENT THROUGH OPINIONS POSTED AS OF June 13, 2008 ***

TITLE 54. Professions, Occupations And Businesses.
CHAPTER 639. Pharmacists and Pharmacy
Prescriptions

Go to the Nevada Code Archive Directory

Nev. Rev. Stat. Ann. § 639.2353 (2008)

639.2353. Transmission of prescription to pharmacist; contents of written prescription; specific directions for use; requirements for written prescription; authentication of prescription given by electronic transmission.

Except as otherwise provided in a regulation adopted pursuant to *NRS 453.385* or *639.2357*:

1. A prescription must be given:

(a) Directly from the practitioner to a pharmacist;

(b) Indirectly by means of an order signed by the practitioner;

(c) By an oral order transmitted by an agent of the practitioner; or

(d) Except as otherwise provided in subsection 5, by electronic transmission or transmission by a facsimile machine, including, without limitation, transmissions made from a facsimile machine to another facsimile machine, a computer equipped with a facsimile modem to a facsimile machine or a computer to another computer, pursuant to the regulations of the board.

2. A written prescription must contain:

(a) Except as otherwise provided in this section, the name and signature of the practitioner, and his address if not immediately available to the pharmacist;

(b) The classification of his license;

(c) The name of the patient, and his address if not immediately available to the pharmacist;

(d) The name, strength and quantity of the drug prescribed;

(e) The symptom or purpose for which the drug is prescribed, if included by the practitioner pursuant to *NRS 639.2352*;

(f) Directions for use; and

85 of 168 DOCUMENTS

*** STATUTES CURRENT THROUGH CHAPTER 392 OF THE 2008 SESSION ***
*** AND CHAPTER 1 OF THE 2008 SPECIAL SESSION ***
*** ANNOTATIONS CURRENT THROUGH CASES DECIDED JULY 11, 2008 ***

TITLE VI Public Officers And Employees
CHAPTER 91-A Access To Governmental Records and Meetings
Procedure for Release of Personal Information for Research Purposes

Go to the New Hampshire Code Archive Directory

RSA 91-A:10 (2008)

91-A:10 Release of Statistical Tables and Limited Data Sets for Research.

I. In this subdivision:

(a) "Agency" means each state board, commission, department, institution, officer or other state official or group.

(b) "Agency head" means the head of any governmental agency which is responsible for the collection and use of any data on persons or summary data.

(c) "Cell size" means the count of individuals that share a set of characteristics contained in a statistical table.

(d) "Data set" means a collection of personal information on one or more individuals, whether in electronic or manual files.

(e) "Direct identifiers" means:

(1) Names.

(2) Postal address information other than town or city, state, and zip code.

(3) Telephone and fax numbers.

(4) Electronic mail addresses.

(5) Social security numbers.

(6) Certificate and license numbers.

(7) Vehicle identifiers and serial numbers, including license plate numbers.

(8) Personal Internet IP addresses and URLs.

(9) Biometric identifiers, including finger and voice prints.

(E) the intended research completion date.

(4) The following information about the data or statistical tables being requested:

(A) general types of information;

(B) time period of the data or statistical tables;

(C) specific data items or fields of information required, if applicable;

(D) medium in which the data or statistical tables are to be supplied; and

(E) any special format or layout of data requested by the principal investigator.

(b) The requestor signs a "Data Use Agreement" signed by the principal investigator that contains the following:

(1) Agreement not to use or further disclose the information to any person or organization other than as described in the application and as permitted by the Data Use Agreement without the written consent of the agency.

(2) Agreement not to use or further disclose the information as otherwise required by law.

(3) Agreement not to seek to ascertain the identity of individuals revealed in the limited data set and/or statistical tables.

(4) Agreement not to publish or make public the content of cells in statistical tables in which the cell size is more than 0 and less than 5 unless:

(A) otherwise provided by law; or

(B) the information is a public record.

(5) Agreement to report to the agency any use or disclosure of the information contrary to the agreement of which the principal investigator becomes aware.

(6) A date on which the data set and/or statistical tables will be returned to the agency and/or all copies in the possession of the requestor will be destroyed.

III. The agency head shall release limited data sets and statistical tables and sign the Data Use Agreement on behalf of the state when:

(a) The application submitted is complete.

(b) Adequate measures to ensure the confidentiality of any person are documented.

(c) The investigator and research staff are qualified as indicated by:

(1) Documentation of training and previous research, including prior publications; and

(2) Affiliation with a university, private research organization, medical center, state agency, or other institution which will provide sufficient research resources.

(d) There is no other state law, federal law, or federal regulation prohibiting release of the requested information.

IV. Within 10 days of a receipt of written application, the agency head, or designee, shall respond to the request.

88 of 168 DOCUMENTS

*** STATUTES CURRENT THROUGH CHAPTER 392 OF THE 2008 SESSION ***
*** AND CHAPTER 1 OF THE 2008 SPECIAL SESSION ***
*** ANNOTATIONS CURRENT THROUGH CASES DECIDED JULY 11, 2008 ***

TITLE XXI Motor Vehicles
CHAPTER 260 Administration of Motor Vehicle Laws
Powers and Duties

Go to the New Hampshire Code Archive Directory

RSA 260:10-b (2008)

260:10-b Collection of Biometric Data Prohibited.

I. The state shall not collect, obtain, or retain any biometric data in connection with motor vehicle registration or operation, or in connection with driver licensing. "Biometric data" includes, but is not limited to:

(a) Fingerprints, palm prints, and other methods for measuring or recording ridge pattern or fingertip characteristics.

(b) Facial feature pattern characteristics.

(c) Behavior characteristics of a handwritten signature, such as shape, speed, pressure, pen angle, or sequence.

(d) Voice data used for comparing live speech with a previously-created speech model of a person's voice.

(e) Iris recognition data containing color or texture patterns or codes.

(f) Keystroke dynamics, measuring pressure applied to key pads.

(g) Hand geometry, measuring hand characteristics, including the shape and length of fingers, in 3 dimensions.

(h) Retinal scans, reading through the pupil to measure blood vessels lining the retina.

(i) DNA/RNA.

II. Paragraph I shall not apply to:

(a) The collection or retention of fingerprints or the purpose of enforcing laws relating to serious traffic offenses, including, but not limited to, driving while intoxicated, reckless driving, negligent homicide with a motor vehicle, operating after being declared an habitual motor vehicle offender, or any motor vehicle offense for which a physical custody arrest was made and bail is required.

(b) The taking or use of signatures, computerized images, likenesses, or photographs, in any form used by the department prior to the effective date of this subparagraph, for licensing purposes, provided that the taking or use is

91 of 168 DOCUMENTS

LexisNexis (TM) New Jersey Annotated Statutes

*** THIS SECTION IS CURRENT THROUGH NEW JERSEY 213TH LEGISLATURE ***
*** FIRST ANNUAL SESSION (P.L. 2008 CH. 97 & J.R. 3) ***
*** ANNOTATIONS CURRENT THROUGH SEPTEMBER 30, 2008 ***

TITLE 39. MOTOR VEHICLES AND TRAFFIC REGULATION
SUBTITLE 1. MOTOR VEHICLES GENERALLY; TRAFFIC LAWS
CHAPTER 2A. NEW JERSEY MOTOR VEHICLE COMMISSION

GO TO THE NEW JERSEY ANNOTATED STATUTES ARCHIVE DIRECTORY

N.J. Stat. § 39:2A-29 (2008)

§ 39:2A-29. Goals of administrator, deputy administrator

The administrator, and the deputy administrator under the direction of the administrator, shall have as their immediate goal the improvement of the safety and security of the State's motor vehicle licensing, registration, titling and inspection system and to this end are authorized to:

a. Make technological improvements, including the modernization of software and hardware, the addition of surveillance cameras, alarms, and access systems, and the utilization of biometrics;

b. Increase the number of audit staff, security guards, and other security-related employees;

c. Improve training and monitoring procedures;

d. Utilize document imaging from the field;

e. Integrate the New Jersey title database with the National Motor Vehicle Title Information System;

f. Improve license plate management, including an automated inventory system and reissuance program;

g. Acquire the ability to access State vital statistics data to immediately update driver's license information;

h. Implement additional proofs of identity verification for a non-driver identification card, driver's license, permits, and registrations;

i. Implement card access systems, clear visibility barriers and door replacements where needed;

j. Replace the written driver's license knowledge test with an online test;

k. Increase the use of credit or debit cards or any other electronic payment device;

l. Increase the use of scanned documents;

m. Match motor vehicle records with Social Security records to verify Social Security numbers in the motor vehicle database, to the extent allowable; and

105 of 168 DOCUMENTS

GENERAL STATUTES OF NORTH CAROLINA

*** THIS DOCUMENT IS CURRENT THROUGH THE 2007 REGULAR SESSION AND 1ST EXTRA SESSION ***
*** ANNOTATIONS CURRENT THROUGH MAY 23, 2008 ***

CHAPTER 130A. PUBLIC HEALTH
ARTICLE 22. A TERRORIST INCIDENT USING NUCLEAR, BIOLOGICAL, OR CHEMICAL AGENTS

Go to the North Carolina Code Archive Directory

N.C. Gen. Stat. § 130A-480 (2008)

§ 130A-480. Emergency department data reporting

(a) For the purpose of ensuring the protection of the public health, the State Health Director shall develop a syndromic surveillance program for hospital emergency departments in order to detect and investigate public health threats that may result from (i) a terrorist incident using nuclear, biological, or chemical agents or (ii) an epidemic or infectious, communicable, or other disease. The State Health Director shall specify the data to be reported by hospitals pursuant to this program, subject to the following:

(1) Each hospital shall submit electronically available emergency department data as specified by rule by the Commission. The Commission, in consultation with hospitals, shall establish by rule a schedule for the implementation of full electronic reporting capability of all data elements by all hospitals. The schedule shall take into consideration the number of data elements already reported by the hospital, the hospital's capacity to electronically maintain the remaining elements, available funding, and other relevant factors.

(2) None of the following data for patients or their relatives, employers, or household members may be collected by the State Health Director: names; postal or street address information, other than town or city, county, state, and the first five digits of the zip code; geocode information; telephone numbers; fax numbers; electronic mail addresses; social security numbers; health plan beneficiary numbers; account numbers; certificate or license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web universal resource locators (URLs); Internet protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

(b) The following are not public records under Chapter 132 of the General Statutes and are privileged and confidential:

(1) Data reported to the State Health Director pursuant to this section.

(2) Data collected or maintained by any entity with whom the State Health Director contracts for the reporting, collection, or analysis of data pursuant to this section.

The State Health Director shall maintain the confidentiality of the data reported pursuant to this section and shall

108 of 168 DOCUMENTS

*** CURRENT THROUGH LEGISLATION PASSED BY THE 127TH OHIO GENERAL ASSEMBLY AND FILED WITH THE SECRETARY OF STATE THROUGH NOVEMBER 3, 2008 ***
*** ANNOTATIONS CURRENT THROUGH SEPTEMBER 1, 2008 ***
*** OPINIONS OF ATTORNEY GENERAL CURRENT THROUGH NOVEMBER 3, 2008 ***

TITLE 37. HEALTH -- SAFETY -- MORALS
CHAPTER 3701. DEPARTMENT OF HEALTH
MISCELLANEOUS

Go to the Ohio Code Archive Directory

ORC Ann. 3701.75 (2008)

§ 3701.75. Standards for using electronic signatures in health care records

(A) As used in this section:

(1) "Electronic record" means a record communicated, received, or stored by electronic, magnetic, optical, or similar means for storage in an information system or transmission from one information system to another. "Electronic record" includes a record that is communicated, received, or stored by electronic data interchange, electronic mail, facsimile, telex, or similar methods of communication.

(2) "Electronic signature" means any of the following attached to or associated with an electronic record by an individual to authenticate the record:

(a) A code consisting of a combination of letters, numbers, characters, or symbols that is adopted or executed by an individual as that individual's electronic signature;

(b) A computer-generated signature code created for an individual;

(c) An electronic image of an individual's handwritten signature created by using a pen computer.

(3) "Health care record" means any document or combination of documents pertaining to a patient's medical history, diagnosis, prognosis, or medical condition that is generated and maintained in the process of the patient's treatment.

(B) All notes, orders, and observations entered into a health care record, including any interpretive reports of diagnostic tests or specific treatments, such as radiologic or electrocardiographic reports, operative reports, reports of pathologic examination of tissue, and similar reports, shall be authenticated by the individual who made or authorized the entry. An entry into a health care record may be authenticated by executing handwritten signatures or handwritten initials directly on the entry. An entry that is an electronic record may be authenticated by an electronic signature if all of the following apply:

1 of 2 DOCUMENTS

OREGON REVISED STATUTES

*** THIS DOCUMENT IS CURRENT THROUGH THE 2007 REGULAR SESSION ***
*** OF THE 74TH LEGISLATIVE ASSEMBLY ***
*** ANNOTATIONS CURRENT THROUGH AUGUST 6, 2008 ***

TITLE 59. OREGON VEHICLE CODE
CHAPTER 807. DRIVING PRIVILEGES AND IDENTIFICATION CARDS
ESTABLISHMENT OF IDENTITY

GO TO OREGON REVISED STATUTES ARCHIVE DIRECTORY

ORS § 807.024 (2007)

Legislative Alert: LEXSEE 2008 Ore. ALS 1 -- See section 14.

807.024. Collection of biometric data; establishment of person's identity; rules; immunity.

(1) A person who applies for issuance, renewal or replacement of a driver license, driver permit or identification card shall submit to collection of biometric data by the Department of Transportation for the purpose of establishing the person's identity. Submitting to collection of biometric data under this section does not excuse a person from responsibility for complying with requirements for proof of identity, age or residence pursuant to ORS 807.050.

(2) For purposes of this section, a person's identity is established if:(a) The department finds that the biometric data collected as required under subsection (1) of this section match the biometric data that are already in the department's records for that person; or

(b) The department finds that the biometric data collected as required under subsection (1) of this section do not match biometric data in the department's records for any other person and the department does not otherwise have reason to believe that the person is not who the person claims to be.

(3) If a person's identity is established as described in subsection (2) of this section, the department shall mail the driver license, driver permit or identification card to the address provided by the person when the person applied for the issuance, renewal or replacement of the license, permit or identification card.

(4) If a person's identity is not established as described in subsection (2) of this section, the department shall:

(a) Inform the person who submitted to collection of biometric data that the person's identity was not established; and

(b) Provide the person with the opportunity to establish the person's identity by an alternative method approved by the department by rule.

(5) If a person's identity was not established as described in subsection (2) of this section and the department has reason to believe that the crime of identity theft, as described in ORS 165.800, was committed by the person currently submitting to collection of biometric data or by a person who previously submitted to collection of biometric data under the identity of the person currently submitting to collection of biometric data, the department shall notify a law enforcement agency that has jurisdiction over the crime.

119 of 168 DOCUMENTS

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS(R)

THIS DOCUMENT IS CURRENT THROUGH 2008 ACTS 1-18, 43, AND 44
TITLES 73 AND 74 CURRENT THROUGH ACTS 1-26, 43, AND 44
*** OCTOBER 3, 2008 ANNOTATION SERVICE ***

PENNSYLVANIA CONSOLIDATED STATUTES
TITLE 4. AMUSEMENTS
PART II. GAMING
CHAPTER 18. FINGERPRINTING

Go to the Pennsylvania Code Archive Directory

4 Pa.C.S. § 1802 (2008)

§ 1802. Submission of fingerprints and photographs

Appointees, employees and prospective employees engaged in the service of the commissions or the board and applicants under this part shall submit to fingerprinting and photographing by the Pennsylvania State Police or by a local law enforcement agency capable of submitting fingerprints and photographs electronically to the Pennsylvania State Police utilizing the Integrated Automated Fingerprint Identification System and the Commonwealth Photo Imaging Network or in a manner and in such form as may be provided by the Pennsylvania State Police. Fingerprinting pursuant to this part shall require, at a minimum, the submission of a full set of fingerprints. Photographing pursuant to this part shall require submission to photographs of the face and any scars, marks or tattoos for purposes of comparison utilizing an automated biometric imaging system. The Pennsylvania State Police shall submit fingerprints when requested by the commissions or the board to the Federal Bureau of Investigation for purposes of verifying the identity of the applicants and obtaining records of criminal arrests and convictions in order to prepare criminal history background investigations under section 1801 (relating to duty to provide). Fingerprints and photographs obtained pursuant to this part may be maintained by the commissions, the board and the Pennsylvania State Police for use pursuant to this part and for general law enforcement purposes. In addition to any other fee or cost assessed by the commissions or the board, an applicant shall pay for the cost of fingerprinting and photographing.

HISTORY: Act 2004-71 (H.B. 2330), § 1, approved July 5, 2004, eff. immediately.; Act 2006-135 (S.B. 862), § 16, approved Nov. 1, 2006, eff. immediately.

SOUTH CAROLINA CODE OF LAWS ANNOTATED BY LEXISNEXIS(R)

*** This document is current through all legislation enacted in 2007 ***
*** Annotations are current through September 2, 2008 ***

TITLE 30. PUBLIC RECORDS
CHAPTER 2. FAMILY PRIVACY PROTECTION ACT

GO TO SOUTH CAROLINA ARCHIVE DIRECTORY

S.C. Code Ann. § 30-2-10 (2007)

Legislative Alert: LEXSEE 2008 S.C. Acts 190 -- See section 3.

§ 30-2-10. Short title.

This chapter shall be designated as the "Family Privacy Protection Act of 2002".

HISTORY: 2002 Act No. 225, § 1.

LexisNexis (R) Notes:

OPINIONS OF ATTORNEY GENERAL

1. [NO NUMBER IN ORIGINAL], *2007 S.C. AG LEXIS 29.*

S.C. Code Ann. § 30-2-20 (2007)

Legislative Alert: LEXSEE 2008 S.C. Acts 190 -- See section 3.

§ 30-2-20. Privacy policies and procedures required of all state entities.

All state agencies, boards, commissions, institutions, departments, and other state entities, by whatever name known, must develop privacy policies and procedures to ensure that the collection of personal information pertaining to citizens of the State is limited to such personal information required by any such agency, board, commission, institution, department, or other state entity and necessary to fulfill a legitimate public purpose.

HISTORY: 2002 Act No. 225, § 1.

LexisNexis (R) Notes:

OPINIONS OF ATTORNEY GENERAL

1. [NO NUMBER IN ORIGINAL], *2007 S.C. AG LEXIS 29.*

S.C. Code Ann. § 30-2-30 (2007)

Legislative Alert: LEXSEE 2008 S.C. Acts 190 -- See section 3.

§ 30-2-30. Definitions.

For purposes of this act, the following terms have the following meanings:

S.C. Code Ann. § 30-2-50 (2007)

Legislative Alert: LEXSEE 2008 S.C. Acts 190 -- See section 3.

§ 30-2-50. Obtaining personal information from state agency for commercial solicitation; penalty

(A) A person or private entity shall not knowingly obtain or use any personal information obtained from a state agency for commercial solicitation directed to any person in this State.

(B) Each state agency shall provide a notice to all requestors of records pursuant to this chapter and to all persons who obtain records pursuant to this chapter that obtaining or using public records for commercial solicitation directed to any person in this State is prohibited.

(C) All state agencies shall take reasonable measures to ensure that no person or private entity obtains or distributes personal information obtained from a public record for commercial solicitation.

(D) A person knowingly violating the provisions of subsection (A) is guilty of a misdemeanor and, upon conviction, must be fined an amount not to exceed five hundred dollars or imprisoned for a term not to exceed one year, or both.

(E) This chapter does not apply to a local governmental entity of a subdivision of this state or local government.

HISTORY: 2002 Act No. 225, § 1; 2003 Act No. 20, § 2.

NOTES:
LexisNexis (R) Notes:
CROSS REFERENCES.--Release of lien filed in error; notification of appropriate parties; prompt action to correct error, see *S.C. Code Ann. § 12-58-160.*

133 of 168 DOCUMENTS

*** This document is current through the 2007 Regular Session ***
* Annotations current through cases posted on lexis.com as of July 27, 2008 *

BUSINESS AND COMMERCE CODE
TITLE 4. MISCELLANEOUS COMMERCIAL PROVISIONS
CHAPTER 35. MISCELLANEOUS
SUBCHAPTER D. MISCELLANEOUS

GO TO TEXAS CODE ARCHIVE DIRECTORY

Tex. Bus. & Com. Code § 35.50 (2007)

§ 35.50. [Repealed April 1, 2009] Biometric Identifier

(a) In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.

(b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person:

(1) informs the individual before capturing the biometric identifier; and

(2) receives the individual's consent to capture the biometric identifier.

(c) A person who possesses a biometric identifier of an individual:

(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(A) the individual consents to the disclosure;

(B) the disclosure completes a financial transaction requested or authorized by the individual;

(C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or

(D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose; and

(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects the person's other confidential information.

(d) A person who violates this section is subject to a civil penalty of not more than $ 25,000 for each violation. The attorney general may institute an action to recover the civil penalty.

HISTORY: Acts 2001, 77th Leg., ch. 634, effective September 1, 2001.

136 of 168 DOCUMENTS

*** This document is current through the 2007 Regular Session ***
* Annotations current through cases posted on lexis.com as of July 27, 2008 *

BUSINESS AND COMMERCE CODE
TITLE 11. PERSONAL IDENTITY INFORMATION
SUBTITLE A. IDENTIFYING INFORMATION
CHAPTER 503. BIOMETRIC IDENTIFIERS

GO TO TEXAS CODE ARCHIVE DIRECTORY

Tex. Bus. & Com. Code § 503.001 (2007)

§ 503.001. [Effective April 1, 2009] Capture or Use of Biometric Identifier

(a) In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.

(b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person:

(1) informs the individual before capturing the biometric identifier; and

(2) receives the individual's consent to capture the biometric identifier.

(c) A person who possesses a biometric identifier of an individual:

(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(A) the individual consents to the disclosure;

(B) the disclosure completes a financial transaction that the individual requested or authorized;

(C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or

(D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose; and

(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses.

(d) A person who violates this section is subject to a civil penalty of not more than $ 25,000 for each violation. The attorney general may bring an action to recover the civil penalty.

HISTORY: Acts 2007, 80th Leg., ch. 885 (H.B. 2278), § 2.01, effective April 1, 2009.

139 of 168 DOCUMENTS

TEXAS STATUTES AND CODES ANNOTATED BY LEXISNEXIS(R)

*** CURRENT THROUGH THE 2007 REGULAR SESSION ***
* Annotations current through cases posted on lexis.com as of June 26, 2008 *

GOVERNMENT CODE
TITLE 4. EXECUTIVE BRANCH
SUBTITLE G. CORRECTIONS
CHAPTER 495. CONTRACTS FOR CORRECTIONAL FACILITIES AND SERVICES
SUBCHAPTER B. MISCELLANEOUS CONTRACTS FOR CORRECTIONAL FACILITIES AND SERVICES

GO TO TEXAS CODE ARCHIVE DIRECTORY

Tex. Gov't Code § 495.025 (2007)

§ 495.025. Inmate Pay Telephone Service [As added by Acts 2007, ch. 100, § 1]

(a) The board shall request proposals from private vendors for a contract to provide pay telephone service to eligible inmates confined in facilities operated by the department. The board may not consider a proposal or award a contract to provide the service unless under the contract the vendor:

(1) provides for installation, operation, and maintenance of the service without any cost to the state;

(2) pays the department a commission of not less than 40 percent of the gross revenue received from the use of any service provided;

(3) provides a system with the capacity to:

(A) compile approved inmate call lists;

(B) verify numbers to be called by inmates, if necessary;

(C) oversee entry of personal identification numbers;

(D) use a biometric identifier of the inmate making the call;

(E) generate reports to department personnel on inmate calling patterns; and

(F) network all individual facility systems together to allow the same investigative monitoring from department headquarters that is available at each facility;

(4) provides on-site monitoring of calling patterns and customizes technology to provide adequate system security;

(5) provides a fully automated system that does not require a department operator;

(6) provides for periodic review by the state auditor of documents maintained by the vendor regarding billing procedures and statements, rate structures, computed commissions, and service metering;

(7) ensures that a ratio of not greater than 30 eligible inmates per communication device is maintained at each facility;

140 of 168 DOCUMENTS

TEXAS STATUTES AND CODES ANNOTATED BY LEXISNEXIS(R)

*** CURRENT THROUGH THE 2007 REGULAR SESSION ***
* Annotations current through cases posted on lexis.com as of June 26, 2008 *

GOVERNMENT CODE
TITLE 4. EXECUTIVE BRANCH
SUBTITLE I. HEALTH AND HUMAN SERVICES
CHAPTER 531. HEALTH AND HUMAN SERVICES COMMISSION
SUBCHAPTER C. MEDICAID AND OTHER HEALTH AND HUMAN SERVICES FRAUD, ABUSE, OR OVERCHARGES

GO TO TEXAS CODE ARCHIVE DIRECTORY

Tex. Gov't Code § 531.1063 (2007)

§ 531.1063. Medicaid Fraud Pilot Program

(a) The commission, with cooperation from the Texas Department of Human Services, shall develop and implement a front-end Medicaid fraud reduction pilot program in one or more counties in this state to address provider fraud and appropriate cases of third-party and recipient fraud.

(b) The program must be designed to reduce:

(1) the number of fraud cases arising from authentication fraud and abuse;

(2) the total amount of Medicaid expenditures; and

(3) the number of fraudulent participants.

(c) The program must include:

(1) participant smart cards and biometric readers that reside at the point of contact with Medicaid providers, recipients, participating pharmacies, hospitals, and appropriate third-party participants;

(2) a secure finger-imaging system that is compliant with the Health Insurance Portability and Accountability Act (HIPAA) and the use of any existing state database of fingerprint images developed in connection with the financial assistance program under Chapter 31, Human Resources Code; fingerprint images collected as part of the program shall only be placed on the smart card; and

(3) a monitoring system.

(d) In implementing the program, the commission may:

(1) exempt recipients who are children or who are elderly or disabled; and

(2) obtain a fingerprint image from a parent or caretaker of a recipient who is a child, regardless of whether the parent or caretaker is a recipient.

(e) The commission must ensure that the procedures for obtaining fingerprint images of participating recipients and

TEXAS STATUTES AND CODES ANNOTATED BY LEXISNEXIS(R)

*** CURRENT THROUGH THE 2007 REGULAR SESSION ***
* Annotations current through cases posted on lexis.com as of June 26, 2008 *

GOVERNMENT CODE
TITLE 5. OPEN GOVERNMENT; ETHICS
SUBTITLE A. OPEN GOVERNMENT
CHAPTER 560. BIOMETRIC IDENTIFIER

GO TO TEXAS CODE ARCHIVE DIRECTORY

Tex. Gov't Code § 560.001 (2007)

§ 560.001. Definitions

In this chapter:

(1) "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.

(2) "Governmental body" has the meaning assigned by Section 552.003, except that the term includes each entity within or created by the judicial branch of state government.

HISTORY: Stats. 2001 77th Leg. Sess. Ch. 634, effective September 1, 2001; Stats. 2003 78th Leg. Sess. Ch. 1275, effective September 1, 2003 (renumbered from Sec. 559.001).

Tex. Gov't Code § 560.002 (2007)

§ 560.002. Disclosure of Biometric Identifier

A governmental body that possesses a biometric identifier of an individual:

(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(A) the individual consents to the disclosure;

(B) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552; or

(C) the disclosure is made by or to a law enforcement agency for a law enforcement purpose; and

(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the governmental body stores, transmits, and protects its other confidential information.

HISTORY: Stats. 2001 77th Leg. Sess. Ch. 634, effective September 1, 2001; Stats. 2003 78th Leg. Sess. Ch. 1275, effective September 1, 2003 (renumbered from Sec. 559.002).

Tex. Gov't Code § 560.003 (2007)

§ 560.003. Application of Chapter 552

A biometric identifier in the possession of a governmental body is exempt from disclosure under Chapter 552.

HISTORY: Stats. 2001 77th Leg. Sess. Ch. 634, effective September 1, 2001; Stats. 2003 78th Leg. Sess. Ch. 1275, effective September 1, 2003 (renumbered from Sec. 559.003).

146 of 168 DOCUMENTS

TEXAS STATUTES AND CODES ANNOTATED BY LEXISNEXIS(R)

*** CURRENT THROUGH THE 2007 REGULAR SESSION ***
* Annotations current through cases posted on lexis.com as of June 26, 2008 *

TRANSPORTATION CODE
TITLE 7. VEHICLES AND TRAFFIC
SUBTITLE B. DRIVER'S LICENSES AND PERSONAL IDENTIFICATION CARDS
CHAPTER 521. DRIVER'S LICENSES AND CERTIFICATES
SUBCHAPTER B. GENERAL LICENSE REQUIREMENTS

GO TO TEXAS CODE ARCHIVE DIRECTORY

Tex. Transp. Code § 521.032 (2007)

§ 521.032. Enhanced Driver's License or Personal Identification Certificate

(a) The department may issue an enhanced driver's license or personal identification certificate for the purposes of crossing the border between this state and Mexico to an applicant who provides the department with proof of United States citizenship, identity, and state residency. If the department issues an enhanced driver's license or personal identification certificate, the department shall continue to issue a standard driver's license and personal identification certificate and offer each applicant the option of receiving the standard or enhanced driver's license or personal identification certificate.

(b) The department shall implement a one-to-many biometric matching system for the enhanced driver's license or personal identification certificate. An applicant for an enhanced driver's license or personal identification certificate must submit a biometric identifier as designated by the department, which, notwithstanding any other law, may be used only to verify the identity of the applicant for purposes relating to implementation of the border crossing initiative established by this section. An applicant must sign a declaration acknowledging the applicant's understanding of the one-to-many biometric match.

(c) The enhanced driver's license or personal identification certificate must include reasonable security measures to protect the privacy of the license or certificate holders, including reasonable safeguards to protect against the unauthorized disclosure of information about the holders. If the enhanced driver's license or personal identification certificate includes a radio frequency identification chip or similar technology, the department shall ensure that the technology is encrypted or otherwise secure from unauthorized information access.

(d) The requirements of this section are in addition to any other requirements imposed on applicants for a driver's license or personal identification certificate. The department shall adopt rules necessary to implement this section. The department shall periodically review technological innovations related to the security of driver's licenses and personal identification certificates and amend the rules as appropriate, consistent with this section, to protect the privacy of driver's license and personal identification certificate holders.

(e) The department may set a fee for issuance of an enhanced driver's license or personal identification certificate in a reasonable amount necessary to implement and administer this section.

(f) The department may enter into a memorandum of understanding with any federal agency for the purposes of facilitating the crossing of the border between this state and Mexico. The department may enter into an agreement with

149 of 168 DOCUMENTS

*** STATUTES CURRENT THROUGH THE 2007 ADJOURNED SESSION (2008) ***
*** ANNOTATIONS CURRENT THROUGH JULY 15, 2008 AND THE APPROPRIATE FEDERAL COURTS THROUGH JUNE 11, 2008 ***

TITLE TWENTY-THREE. MOTOR VEHICLES
CHAPTER 9. OPERATORS' LICENSES
SUBCHAPTER 2. EXAMINATIONS

Go to the Vermont Code Archive Directory

23 V.S.A. § 634 (2007)

§ 634. Fee for examination

(a) The fee for an examination for a learner's permit shall be $ 25.00. The fee for an examination to obtain an operator's license when the applicant is required to pass an examination pursuant to section 632 of this title shall be $ 15.00.

(b) The department of motor vehicles shall not implement any procedures or processes for identifying applicants for licenses, learner permits, or nondriver identification cards that involve the use of biometric identifiers. Pursuant to the provisions of *49 U.S.C. § 31308,* this subsection shall not apply to applicants for commercial driver licenses or endorsements on these licenses.

HISTORY: Amended 1975, No. 193 (Adj. Sess.), § 3; 1989, No. 51, § 39; 2001, No. 102 (Adj. Sess.), § 24, eff. May 15, 2002; 2003, No. 154 (Adj. Sess.), § 12; 2005, No. 175 (Adj. Sess.), § 36.

NOTES:
HISTORY

SOURCE. V.S. 1947, § 10,147. P.L. § 5096. 1927, No. 74, § 10. 1927, No. 69, § 2. 1925, No. 70, § 45.

AMENDMENTS--2005 (ADJ. SESS.). Subsection (a): Substituted "$25.00" for "$20.00" in the first sentence, and "$15.00" for "$5.00" in the second sentence.

--2003 (ADJ. SESS.). Designated existing provisions of section as subsec. (a), amended subsec. (a) generally, and added subsec. (b).

--2001 (ADJ. SESS.). Substituted "$20.00" for "$15.00" and "$15.00" for "$10.00" in the first sentence.

--1989. Substituted "$15.00" for "$10.00" preceding "for the first examination, and" and "$10.00" for "$5.00" thereafter.

--1975 (ADJ. SESS.). Substituted "$10.00 for the first examination, and $5.00 for any additional examination" for "$2.00" preceding "and shall be paid" in the first sentence.

CODE OF VIRGINIA

*** CURRENT THROUGH THE 2008 REGULAR SESSION, Acts 2008, cc. 1 to 884,
2008 Special Session I, cc. 1 and 2. ***
*** 2008 Special Session II, cc. 1 to 11 ***
*** ANNOTATIONS CURRENT THROUGH JUNE 30, 2008 ***

TITLE 2.2. ADMINISTRATION OF GOVERNMENT
SUBTITLE II. ADMINISTRATION OF STATE GOVERNMENT
PART B. TRANSACTION OF PUBLIC BUSINESS
CHAPTER 38. GOVERNMENT DATA COLLECTION AND DISSEMINATION PRACTICES ACT

GO TO CODE OF VIRGINIA ARCHIVE DIRECTORY

Va. Code Ann. § 2.2-3800 (2008)

§ 2.2-3800. Short title; findings; principles of information practice

A. This chapter may be cited as the "Government Data Collection and Dissemination Practices Act."

B. The General Assembly finds that:

1. An individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;

2. The increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;

3. An individual's opportunities to secure employment, insurance, credit, and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems; and

4. In order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals.

C. Recordkeeping agencies of the Commonwealth and political subdivisions shall adhere to the following principles of information practice to ensure safeguards for personal privacy:

1. There shall be no personal information system whose existence is secret.

2. Information shall not be collected unless the need for it has been clearly established in advance.

3. Information shall be appropriate and relevant to the purpose for which it has been collected.

4. Information shall not be obtained by fraudulent or unfair means.

5. Information shall not be used unless it is accurate and current.

6. There shall be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination.

7. There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.

8. Any agency holding personal information shall assure its reliability and take precautions to prevent its misuse. On and after July 1, 2004, no agency shall display the social security number of a data subject on a student or employee identification card, except that for universities and colleges that have such a prevention plan for misuse of personal information in place on or before July 1, 2004, in compliance with this section, the date shall be January 1, 2005. On and after July 1, 2006, no agency shall display an individual's entire social security number on any student or employee identification card.

DESIGN, ESTABLISHMENT, AND MAINTENANCE OF A SECURE DATA PROCESSING SYSTEM CONTAINING CONFIDENTIAL TAXPAYER INFORMATION primarily is a question of fact to be determined by the local commissioner of the revenue; further, the commissioner should balance his administrative discretion with the prohibitions and restrictions contained in this section and the Government Data Collection and Dissemination Practices Act. See opinion of Attorney General to The Honorable Ray Ergenbright, Commissioner of the Revenue for the City of Staunton, 05-021 (6/14/05).

DESIGN AND CONSTRUCTION OF A DATA PROCESSING SYSTEM CONTAINING CONFIDENTIAL TAXPAYER INFORMATION WITHOUT ACCESS TO THE DATA is not necessarily subject to the secrecy provisions of *§ 58.1-3*, which prohibits a commissioner from divulging certain information obtained in the performance of his duties. See opinion of Attorney General to The Honorable Ray Ergenbright, Commissioner of the Revenue for the City of Staunton, 05-021 (6/14/05).

Va. Code Ann. § 2.2-3801 (2008)

THIS SECTION HAS MORE THAN ONE DOCUMENT WITH VARYING EFFECTIVE DATES.

§ 2.2-3801. (Effective until July 1, 2009) Definitions

As used in this chapter, unless the context requires a different meaning:

1. *"Information system"* means the total components and operations of a record-keeping process, including information collected or managed by means of computer networks and the Internet, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.

2. *"Personal information"* means all information that describes, locates or indexes anything about an individual including his real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. "Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information.

3. *"Data subject"* means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system.

4. *"Disseminate"* means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means.

5. *"Purge"* means to obliterate information completely from the transient, permanent, or archival records of an organization.

6. *"Agency"* means any agency, authority, board, department, division, commission, institution, bureau, or like governmental entity of the Commonwealth or of any unit of local government including counties, cities, towns, regional governments, and the departments thereof, and includes constitutional officers, except as otherwise expressly provided by law. "Agency" shall also include any entity, whether public or private, with which any of the foregoing has entered into a contractual relationship for the operation of a system of personal information to accomplish an agency function. Any such entity included in this definition by reason of a contractual relationship shall only be deemed an agency as relates to services performed pursuant to that contractual relationship, provided that if any such entity is a consumer reporting agency, it shall be deemed to have satisfied all of the requirements of this chapter if it fully complies with the requirements of the Federal Fair Credit Reporting Act as applicable to services performed pursuant to such contractual relationship.

HISTORY: 1976, c. 597, § 2.1-379; 1983, c. 372; 1999, c. 41; 2001, c. 844; 2003, c. 272; 2006, c. 474.

NOTES:

ter if it fully complies with the requirements of the Federal Fair Credit Reporting Act as applicable to services performed pursuant to such contractual relationship.

"Data subject" means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system.

"Disseminate" means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means.

"Information system" means the total components and operations of a record-keeping process, including information collected or managed by means of computer networks and the Internet, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.

"Personal information" means all information that (i) describes, locates or indexes anything about an individual including, but not limited to, his social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or (ii) affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. "Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information.

"Purge" means to obliterate information completely from the transient, permanent, or archival records of an organization.

HISTORY: 1976, c. 597, § 2.1-379; 1983, c. 372; 1999, c. 41; 2001, c. 844; 2003, c. 272; 2006, c. 474; 2008, cc. 840, 843.

NOTES:

SECTION SET OUT TWICE. --The section above is effective July 1, 2009. For the version of this section effective until July 1, 2009, see the preceding section, also numbered 2.2-3801.

EDITOR'S NOTE. --Acts 2008, cc. 840 and 843, cl. 2 provides: "That the provisions of this act shall become effective on July 1, 2009, except that the third and fourth enactments of this act shall become effective on July 1, 2008."

Acts 2008, cc. 840 and 843, cl. 3 provides: "That every state agency subject to the provisions of the Government Data Collection and Dissemination Practices Act (*§ 2.2-3800* et seq.) shall conduct an analysis and review of its collection and use of social security numbers, to be completed by October 1, 2008. Each such agency shall submit, no later than October 1, 2008, to the chairmen of the Freedom of Information Advisory Council and the Joint Commission on Technology and Science, on forms developed by the Council and the Commission, (i) a list of (a) all state or federal statutes authorizing or requiring the collection of social security numbers by such agency and (b) instances where social security numbers are voluntarily collected or (ii) in the absence of statutory authority to collect social security numbers, written justification explaining why continued collection is essential to its transaction of public business. In conducting such a review, each agency shall be encouraged to consider whether such collection and use is essential for its transaction of public business and to find alternative means of identifying individuals. The chairmen of the Council and the Commission may withhold from public disclosure any such lists or portions of lists as legislative working papers, if it deems that the public dissemination of such lists or portions of lists would cause a potential invasion of privacy."

Acts 2008, cc. 840 and 843, cl. 4 provides: "That every county and city, and any town with a population in excess of 15,000 shall, no later than September 10, 2008, provide the Virginia Municipal League or the Virginia Association of Counties, as appropriate, information on a form agreed upon by the Virginia Municipal League, the Virginia Association of Counties and staff of the Freedom of Information Advisory Council and the Joint Commission on Technology and Science identifying (i) all state or federal statutes authorizing or requiring the collection of social security numbers by such county, city or town and (ii) instances where social security numbers are voluntarily collected or (iii) in the absence of statutory authority to collect social security numbers, written justification explaining why continued collection is essential to its transaction of public business. In conducting such a review, each such county, city or town shall be encouraged to consider whether such collection and use is essential for its transaction of public business and to find alternative means of identifying individuals. The information required by this enact-

12. Maintained by the Department of the State Internal Auditor or internal audit departments of state agencies or institutions that deal with communications and investigations relating to the State Employee Fraud, Waste and Abuse Hotline.

HISTORY: 1976, c. 597, § 2.1-384; 1979, c. 685; 1980, c. 752; 1981, cc. 461, 464, 504, 589; 1982, c. 225; 1983, c. 289; 1984, c. 750; 1986, c. 62; 1990, c. 825; 1992, c. 620; 1993, cc. 205, 963; 1996, cc. 154, 590, 598, 952; 2001, c. 844; 2003, c. 406; 2005, cc. 868, 881; 2006, cc. 196, 857, 914.

NOTES:

EDITOR'S NOTE. --Acts 2006, c. 857, cl. 4, provides: "That the provisions of this act may result in a net increase in periods of imprisonment or commitment. Pursuant to *§ 30-19.1:4*, the estimated amount of the necessary appropriation is $2,419,496 for periods of imprisonment in state adult correctional facilities and is $0 for periods of commitment to the custody of the Department of Juvenile Justice."

Acts 2006, c. 914, cl. 5, provides: "That the provisions of this act may result in a net increase in periods of imprisonment or commitment. Pursuant to *§ 30-19.1:4*, the estimated amount of the necessary appropriation is at least $2,419,496 for periods of imprisonment in state adult correctional facilities and is $0 for periods of commitment to the custody of the Department of Juvenile Justice."

THE 2003 AMENDMENTS. --The 2003 amendment by c. 406 inserted "the Virginia Racing Commission" in subdivision 6.

THE 2005 AMENDMENTS. --The 2005 amendments by cc. 868 and 881 are identical, and in subdivision 10, substituted "Department of Forensic Science" for "Division of Forensic Science of the Department of Criminal Justice Services," and "9.1-1104" for "9.1-121."

THE 2006 AMENDMENTS. --The 2006 amendment by c. 196 inserted "the police department of the Chesapeake Bay Bridge and Tunnel Commission" in subdivision 7.

The 2006 amendments by cc. 857 and 914 are identical, and added the language beginning "or in the Sex Offender and Crimes Against Minors Registry" to the end of subdivision 3.

LAW REVIEW. --For article discussing decisions of Virginia courts dealing with state administrative procedures between June 1, 2002 and June 1, 2003, see U. Rich. L. Rev. 39 (2003).

Va. Code Ann. § 2.2-3803 (2008)

§ 2.2-3803. Administration of systems including personal information; Internet privacy policy; exceptions

A. Any agency maintaining an information system that includes personal information shall:

1. Collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency;

2. Collect information to the greatest extent feasible from the data subject directly;

3. Establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

4. Maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to ensure fairness in determinations relating to a data subject;

5. Make no dissemination to another system without (i) specifying requirements for security and usage including limitations on access thereto, and (ii) receiving reasonable assurances that those requirements and limitations will be observed. This subdivision shall not apply, however, to a dissemination made by an agency to an agency in another state, district or territory of the United States where the personal information is requested by the agency of such other state, district or territory in connection with the application of the data subject therein for a

LAW REVIEW. --For survey on legal issues involving children in Virginia for 1989, see *23 U. Rich. L. Rev. 705 (1989).*

CHAPTER DOES NOT RENDER PERSONAL INFORMATION CONFIDENTIAL. Indeed, the act does not generally prohibit the dissemination of information. Instead, it requires certain procedural steps to be taken in the collection, maintenance, use, and dissemination of such data. *Hinderliter v. Humphries, 224 Va. 439, 297 S.E.2d 684 (1982)* (decided under former Title 2.1).

BURDEN IS ON PLAINTIFF TO ESTABLISH LACK OF NECESSITY OR IMPROPER PURPOSE FOR DISSEMINATION. Hinderliter v. Humphries, 224 Va. 439, 297 S.E.2d 684 (1982) (decided under former Title 2.1).

SINCE PUBLIC OFFICIALS PRESUMED TO OBEY THE LAW. --There is a presumption that public officials will obey the law, and there is nothing in this act that reverses such presumption or imposes the ultimate burden of proof on defendants sued under it. Consequently, the presumption stands until rebutted by contrary evidence. *Hinderliter v. Humphries, 224 Va. 439, 297 S.E.2d 684 (1982)* (decided under former Title 2.1).

THE GOVERNMENT DATA COLLECTION AND DISSEMINATION PRACTICES ACT, DOES NOT APPLY TO CONSTITUTIONAL OFFICERS. --Constitutional officer does not come within the definition of "agency" in *§ 2.2-3801*, therefore, the act did not apply to a city treasurer who allegedly gave a newspaper reporter information from a former city employee's employment file, and the city treasurer did not violate subdivision A 1 of *§ 2.2-3803. Carraway v. Hill, 265 Va. 20, 574 S.E.2d 274, 2003 Va. LEXIS 7 (2003)* (decided prior to 2003 amendment to *§ 2.2-3801*).

CIRCUIT COURT OPINIONS

FREEDOM OF INFORMATION ACT REQUESTS. --Names of individual claimants were not protected by *§ 2.2-3803* under the Virginia Government Data Collection and Dissemination Practices Act, where a reporter requested from a city information about claims against the city. *Davis v. City of Chesapeake, 74 Va. Cir. 367, 2007 Va. Cir. LEXIS 299 (Chesapeake 2007).*

EMPLOYMENT RECORD. --Because a report and investigatory materials were related to an employee's employment record and because the report plainly involved an employment discrimination complaint about things done by the employee that adversely affected him, *§ 2.2-3803* of the Virginia Government Data Collection and Dissemination Act, required disclosure by the county to the employee of that personal information, including the identity of the complainants, informants, and others involved in the investigation. *McChrystal v. Fairfax County Bd. of Supervisors, 67 Va. Cir. 171, 2005 Va. Cir. LEXIS 26 (Fairfax County 2005).*

Va. Code Ann. § 2.2-3804 (2008)

§ 2.2-3804. Military recruiters to have access to student information, school buildings, etc

If a public school board or public institution of higher education provides access to its buildings and grounds and the student information directory to persons or groups that make students aware of occupational or educational options, the board or institution shall provide access on the same basis to official recruiting representatives of the armed forces of the Commonwealth and the United States for the purpose of informing students of educational and career opportunities available in the armed forces.

HISTORY: 1981, c. 377, § 2.1-380.1; 2001, c. 844.

under the Virginia Freedom of Information Act (*§ 2.2-3700* et seq.) or within a time period as may be mutually agreed upon by the agency and the data subject.

b. The disclosures to data subjects required under this chapter shall be made (i) in person, if he appears in person and furnishes proper identification, or (ii) by mail, if he has made a written request, with proper identification. Copies of the documents containing the personal information sought by a data subject shall be furnished to him or his representative at reasonable charges for document search and duplication in accordance with subsection F of *§ 2.2-3704.*

c. The data subject shall be permitted to be accompanied by a person of his choosing, who shall furnish reasonable identification. An agency may require the data subject to furnish a written statement granting the agency permission to discuss the individual's file in such person's presence.

5. If the data subject gives notice that he wishes to challenge, correct, or explain information about him in the information system, the following minimum procedures shall be followed:

a. The agency maintaining the information system shall investigate, and record the current status of that personal information.

b. If, after such investigation, the information is found to be incomplete, inaccurate, not pertinent, not timely, or not necessary to be retained, it shall be promptly corrected or purged.

c. If the investigation does not resolve the dispute, the data subject may file a statement of not more than 200 words setting forth his position.

d. Whenever a statement of dispute is filed, the agency maintaining the information system shall supply any previous recipient with a copy of the statement and, in any subsequent dissemination or use of the information in question, clearly note that it is disputed and supply the statement of the data subject along with the information.

e. The agency maintaining the information system shall clearly and conspicuously disclose to the data subject his rights to make such a request.

f. Following any correction or purging of personal information the agency shall furnish to past recipients notification that the item has been purged or corrected whose receipt shall be acknowledged.

B. Nothing in this chapter shall be construed to require an agency to disseminate any recommendation or letter of reference from or to a third party that is a part of the personnel file of any data subject nor to disseminate any test or examination used, administered or prepared by any public body for purposes of evaluation of (i) any student or any student's performance, (ii) any seeker's qualifications or aptitude for employment, retention, or promotion, or (iii) qualifications for any license or certificate issued by any public body.

As used in this subsection, "test or examination" includes (i) any scoring key for any such test or examination and (ii) any other document that would jeopardize the security of the test or examination. Nothing contained in this subsection shall prohibit the release of test scores or results as provided by law, or to limit access to individual records as provided by law; however, the subject of the employment tests shall be entitled to review and inspect all documents relative to his performance on those employment tests.

When, in the reasonable opinion of the public body, any such test or examination no longer has any potential for future use, and the security of future tests or examinations will not be jeopardized, the test or examination shall be made available to the public. Minimum competency tests administered to public school children shall be made available to the public contemporaneously with statewide release of the scores of those taking such tests, but in no event shall such tests be made available to the public later than six months after the administration of such tests.

C. Neither any provision of this chapter nor any provision of the Freedom of Information Act (*§ 2.2-3700* et seq.) shall be construed to deny public access to records of the position, job classification, official salary or rate of pay of, and to records of the allowances or reimbursements for expenses paid to any public officer, official or employee at any level of state, local or regional government in the Commonwealth. The provisions of this subsection shall not apply to records of the official salaries or rates of pay of public employees whose annual rate of pay is $ 10,000 or less.

D. Nothing in this section or in this chapter shall be construed to require an agency to disseminate information derived from tax returns in violation of *§§ 2.2-3705.7* and *58.1-3.*

HISTORY: 1976, c. 597, § 2.1-385; 2001, c. 844; 2003, c. 974.

NOTES:
SECTION SET OUT TWICE. --The section above is effective until July 1, 2009. For the version of this section effective July 1, 2009, see the following section, also numbered 2.2-3808.

THE 2003 AMENDMENTS. --The 2003 amendment by c. 974 inserted the subsection A designation; and added subsections B through D.

EDITOR'S NOTE. --The case below was decided under former Title 2.1 or prior provisions.

FEDERAL COURT COULD NOT HEAR CLAIM UNDER THIS SECTION against local registrar and state election officials for conditioning voting on disclosure of social security number where none of the exceptions to the Eleventh Amendment's bar against federal jurisdiction were present. The state did not waive its immunity and consent to suit, nor could defendants' actions be classified as beyond the scope of their statutory authority. *Greidinger v. Davis, 782 F. Supp. 1106 (E.D. Va. 1992),* rev'd on other grounds, *988 F.2d 1344 (4th Cir. 1993).*

Va. Code Ann. § 2.2-3808 (2008)

THIS SECTION HAS MORE THAN ONE DOCUMENT WITH VARYING EFFECTIVE DATES.

§ 2.2-3808. (Effective July 1, 2009) Collection, disclosure, or display of social security number

A. No agency shall require an individual to furnish or disclose his social security number or driver's license number unless the furnishing or disclosure of such number is (i) authorized or required by state or federal law and (ii) essential for the performance of that agency's duties. Nor shall any agency require an individual to disclose or furnish his social security account number not previously disclosed or furnished, for any purpose in connection with any activity, or to refuse any service, privilege or right to an individual wholly or partly because the individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by federal or state law.

B. Agency-issued identification cards, student identification cards, or license certificates issued or replaced on or after July 1, 2003, shall not display an individual's entire social security number except as provided in *§ 46.2-703.*

C. Any agency-issued identification card, student identification card, or license certificate that was issued prior to July 1, 2003, and that displays an individual's entire social security number shall be replaced no later than July 1, 2006, except that voter registration cards issued with a social security number and not previously replaced shall be replaced no later than the December 31st following the completion by the state and all localities of the decennial redistricting following the 2010 census. This subsection shall not apply to (i) driver's licenses and special identification cards issued by the Department of Motor Vehicles pursuant to Chapter 3 (*§ 46.2-300* et seq.) of Title 46.2 and (ii) road tax registrations issued pursuant to *§ 46.2-703.*

D. The provisions of subsections A and C shall not be applicable to licenses issued by the State Corporation Commission's Bureau of Insurance until such time as a national insurance producer identification number has been created and implemented in all states. Commencing with the date of such implementation, the licenses issued by the State Corporation Commission's Bureau of Insurance shall be issued in compliance with subsection A of this section. Further, all licenses issued prior to the date of such implementation shall be replaced no later than 12 months following the date of such implementation.

HISTORY: 1976, c. 597, § 2.1-385; 2001, c. 844; 2003, c. 974; 2008, cc. 840, 843.

NOTES:
SECTION SET OUT TWICE. --The section above is effective July 1, 2009. For the version of this section effective until July 1, 2009, see the preceding section, also numbered 2.2-3808.

THE 2007 AMENDMENTS. --The 2007 amendments by cc. 548 and 626 are identical, and deleted "or *§ 2.2-3802*" following "this title" and deleted "or court clerk" following "agency" three times in the first sentence.

Va. Code Ann. § 2.2-3808.2 (2008)

§ 2.2-3808.2.

Repealed by Acts 2007, cc. 548 and 626, cl. 5.

NOTES:
CROSS REFERENCES. --For current provisions as to posting and availability of certain information on the Internet, see *§ 17.1-293*.

[Repealed]

Va. Code Ann. § 2.2-3809 (2008)

THIS SECTION HAS MORE THAN ONE DOCUMENT WITH VARYING EFFECTIVE DATES.

§ 2.2-3809. (Effective until July 1, 2009) Injunctive relief; attorneys' fees

Any aggrieved person may institute a proceeding for injunction or mandamus against any person or agency that has engaged, is engaged, or is about to engage in any acts or practices in violation of the provisions of this chapter. The proceeding shall be brought in the circuit court of any county or city wherein the person or agency made defendant resides or has a place of business.

In the case of any successful proceeding by an aggrieved party, the person or agency enjoined or made subject to a writ of mandamus by the court shall be liable for the costs of the action together with reasonable attorneys' fees as determined by the court.

HISTORY: 1976, c. 597, § 2.1-386; 2001, c. 844.

NOTES:
SECTION SET OUT TWICE. --The section above is effective until July 1, 2009. For the version of this section effective July 1, 2009, see the following section, also numbered 2.2-3809.

ONLY REMEDY FOR VIOLATION OF THIS CHAPTER IS SET FORTH IN THIS SECTION. Hinderliter v. Humphries, 224 Va. 439, 297 S.E.2d 684 (1982) (decided under former Title 2.1).

PLAINTIFF RELIEVED OF NORMAL BURDEN OF PROOF. --This section relieves plaintiff of the normal burden of proving that an adequate remedy at law does not exist and that irreparable injury will occur. *Hinderliter v. Humphries, 224 Va. 439, 297 S.E.2d 684 (1982)* (decided under former Title 2.1).

DAMAGES NOT RECOVERABLE UNDER ACT. --Only injunctive relief and mandamus are available under this act, and a claim for damages is, accordingly, subject to being stricken. *Mansoor v. County of Albemarle, 124 F. Supp. 2d 367, 2000 U.S. Dist. LEXIS 18612 (W.D. Va. 2000)* (decided under former Title 2.1).

"ANY PERSON" REFERS TO PERSONS THROUGH WHOM COVERED AGENCIES CONDUCT THEIR BUSINESS. --Phrase "any person" in *§ 2.2-3809* refers to those persons through whom covered agencies conduct their business; a city treasurer, who was a constitutional officer, did not come within that phrase. *Carraway v. Hill, 265 Va. 20, 574 S.E.2d 274, 2003 Va. LEXIS 7 (2003)* (decided prior to 2003 amendment to *§ 2.2-3801*).

ment shall be submitted no later than October 1, 2008 to the chairmen of the Freedom of Information Advisory Council and the Joint Commission on Technology and Science, on forms developed by the Council and the Commission."

THE 2008 AMENDMENTS. --The 2008 amendments by cc. 840 and 843, effective July 1, 2009, are identical, and in the first paragraph, inserted "district or" and substituted "where the aggrieved person resides or where the agency made defendant has a place of business" for "wherein the person or agency made defendant resides or has a place of business" at the end of the second sentence; in the second paragraph, deleted "person or" preceding "agency enjoined"; and added the last paragraph.

153 of 168 DOCUMENTS

*** STATUTES CURRENT THROUGH ALL NEW 2008 LEGISLATION ***
*** ANNOTATIONS CURRENT THROUGH JUNE 30, 2008 ***

TITLE 46. MOTOR VEHICLES
CHAPTER 46.20. DRIVERS' LICENSES -- IDENTICARDS
ARTICLE 1. DRIVER'S LICENSE AND PERMIT REQUIREMENTS

GO TO REVISED CODE OF WASHINGTON ARCHIVE DIRECTORY

Rev. Code Wash. (ARCW) § 46.20.037 (2008)

§ 46.20.037. Biometric matching system -- Administration -- Exception

(1) No later than two years after full implementation of the provisions of Title II of P.L. 109-13, improved security for driver's licenses and personal identification cards (Real ID), as passed by Congress May 10, 2005, the department shall implement a voluntary biometric matching system for driver's licenses and identicards. A biometric matching system shall be used only to verify the identity of an applicant for a renewal or duplicate driver's license or identicard by matching a biometric identifier submitted by the applicant against the biometric identifier submitted when the license was last issued. This project requires a full review by the information services board using the criteria for projects of the highest visibility and risk.

(2) Any biometric matching system selected by the department shall be capable of highly accurate matching, and shall be compliant with biometric standards established by the American association of motor vehicle administrators.

(3) The biometric matching system selected by the department must incorporate a process that allows the owner of a driver's license or identicard to present a personal identification number or other code along with the driver's license or identicard before the information may be verified by a third party, including a governmental entity.

(4) Upon the establishment of a biometric driver's license and identicard system as described in this section, the department shall allow every person applying for an original, renewal, or duplicate driver's license or identicard to voluntarily submit a biometric identifier. Each applicant shall be informed of all ways in which the biometric identifier may be used, all parties to whom the identifier may be disclosed and the conditions of disclosure, the expected error rates for the biometric matching system which shall be regularly updated as the technology changes or empirical data is collected, and the potential consequences of those errors. The department shall adopt rules to allow applicants to verify the accuracy of the system at the time that biometric information is submitted, including the use of at least two separate devices.

(5) The department may not disclose biometric information to the public or any governmental entity except when authorized by court order.

(6) All biometric information shall be stored with appropriate safeguards, including but not limited to encryption.

157 of 168 DOCUMENTS

*** Text Current Through 2008 Regular and 1st and 2nd Extraordinary Sessions ***
*** Annotations Current Through August 18, 2008 ***

Chapter 17B. Motor Vehicle Driver's Licenses.
Article 2. Issuance of License, Expiration and Renewal.

GO TO WEST VIRGINIA STATUTES ARCHIVE DIRECTORY

W. Va. Code § 17B-2-12a (2008)

§ 17B-2-12a. Renewal of driver's license upon expiration; vision screening; renewal fees.

(a) The commissioner shall notify each person who holds a valid driver's license of the expiration date of the license by first class mail to the last address known to the division. The notice shall be mailed at least ninety days prior to the expiration date of the license and shall include a renewal application form and instructions for renewal.

(b) The holder of a valid driver's license may apply to the division for renewal of the license on the form provided by the division. To be eligible for license renewal the applicant must:

(1) Pay the fee required by section eight [*§ 17B-2-8*] of this article;

(2) Obtain a new color photograph from the division; and

(3) Pass a vision screening conducted by the division.

(c) The commissioner shall assess an additional fee of five dollars for every application for renewal submitted after the expiration of the applicant's license.

(d) The commissioner shall determine whether an applicant qualifies for a renewed license.

(e) The commissioner shall provide by rule a procedure by which an applicant who does not meet the minimum vision standards for licensure may present evidence to show that his or her vision has been corrected to meet the minimum visual standards and that he or she is capable of safely operating a motor vehicle.

(f) The commissioner may not renew the driver's license of an applicant whose eyesight cannot be corrected to conform to the minimum vision standards established by this code and by the rules of the commissioner.

(g) Vision screening conducted pursuant to this section shall not be used to collect any type of personal biometric identifying information including, but not limited to, a retinal scan.

(h) The commissioner shall propose legislative rules for promulgation in accordance with the provisions of article three [*§§ 29A-3-1* et seq.], chapter twenty-nine-a of this code to implement the provisions of this section.

(i) The provisions of this section requiring an applicant for renewal of a driver's license to successfully complete a