

Summary of Legislation

This bill makes changes related to the handling of personally identifying information and required procedures and notifications if this information is breached.

Record disposal policy. This bill requires each public and private entity in the state that maintains paper or electronic documents that contain personally identifying information to develop a written policy for the disposal of such records. Unless otherwise required by federal law, this policy must require the destruction of these records in a manner that ensures the personally identifying information is unreadable through any means.

Security procedures and breach notification. A person that maintains, owns, or licenses personally identifying information or uses a third party as a service provider must implement and maintain appropriate security procedures to protect personally identifying information from unauthorized access.

This bill adds definitions related to the disclosure of a security breach and requires an individual or commercial entity to give notice to affected Colorado residents upon discovery of a security breach as soon as possible, but no later than 45 days from the date of the breach. This bill describes what information must be included in such a notification including, but not limited to, the date of the breach, a description of the information accessed in the breach, and information for contacting credit agencies and the Federal Trade Commission. Individuals and commercial entities are prohibited from charging for the cost of providing this notice.

Breach reporting to the Attorney General. An individual or commercial entity is required to provide notice to the Colorado Attorney General within seven days if unencrypted or encrypted computerized data is breached and the breach is believed to impact 500 or more Colorado residents. The Attorney General is authorized to investigate and prosecute the breach upon receipt of this notice.

Background

As defined under current law, in the Colorado Consumer Protection Act, a person is an individual, corporation, business trust, estate, trust, partnership, or unincorporated association. Under current law, a person breaching computerized data can be charged with a misdemeanor or felony depending on the nature of the crime.

Assumptions

For this analysis, all state and local government agencies were canvassed and the majority responded that they already have document disposal requirements that are in compliance with the requirements established for public entities under this bill. Therefore, this analysis assumes that most agencies can implement this bill within existing appropriations. To the extent that an agency requires additional appropriations, it is assumed they will be requested through the annual budget process.

State Revenue

Beginning in FY 2018-19, this bill may increase state revenue from criminal fines and court administrative fees by less than \$5,000 per year.

Criminal fines. To the extent that reporting breaches to the Colorado Attorney General increases the number of computer crime offenses prosecuted, this bill will increase state revenue credited to the Fines Collection Cash Fund in the Judicial Department. It is unknown if these will be misdemeanor or felony computer crime offenses. Depending on the nature of the crime, a computer crime can range from a petty 1 misdemeanor to a class 2 felony with a fine penalty range of no more than \$500 (petty 1 misdemeanor) up to \$1.0 million (class 2 felony). Because the courts have the discretion of incarceration, imposing a fine, or both, the precise impact to state revenue cannot be determined, but is assumed to be minimal and less than \$5,000 per year.

Court and administrative fees. The bill may also increase state fee revenue by an amount credited to the General Fund and various cash funds. Fees are imposed for a variety of court-related costs, which vary based on the offense but may include probation supervision, drug or sex offender surcharges, victim compensation, and late fees, among others. Some fee revenue is shared with local governments; refer to the Local Government Impact section for additional information.

TABOR Refund

The bill may increase state cash fund revenue from criminal fines and fees subject to TABOR in FY 2018-19 and FY 2019-20 by less than \$5,000 per year. State revenue is not currently expected to exceed the TABOR limit in either year and no refund is required. Therefore, the bill is not expected to impact TABOR refunds in these years. However, refunds in future years when the state next collects a TABOR surplus may be increased.

State Expenditures

This bill increases state General Fund expenditures in the Department of Personnel and Administration by \$11,627 and 0.2 FTE in FY 2018-19 and \$16,986 and 0.3 FTE in FY 2019-20. This bill also increases state agency workload. These impacts are shown in Table 2 and described below.

Table 2
Expenditures Under HB 18-1128

	FY 2018-19	FY 2019-20
Department of Personnel and Administration		
Personal Services	\$9,157	\$13,318
Centrally Appropriated Costs*	\$2,470	\$3,668
FTE – Personal Services	0.2 FTE	0.3 FTE
Total Cost	\$11,627	\$16,986
Total FTE	0.2 FTE	0.3 FTE

* Centrally appropriated costs are not included in the bill's appropriation.

Department of Personnel and Administration. The Colorado State Archives section of the Department of Personnel and Administration serves as the official repository of permanent state records for all state agencies. It is assumed that an archivist will spend an additional 667 hours per year or 0.3 FTE on an ongoing basis redacting records to ensure personally identifying information is unreadable as a result of this bill. Costs in year one are prorated due to the effective date of the bill.

Department of Law. This bill increases workload in the Consumer Protection Section of the Department of Law to receive data breach notifications from individual or commercial entities that experience a breach of data effecting over 500 Colorado residents. Because data breach notices are currently provided to the department on a voluntary basis, it is assumed that this workload increase will be minimal and can be accomplished within existing appropriations. Workload also increases to investigate and prosecute data breach computer crimes. The number of crimes requiring investigation is unknown and it is assumed the department will request an increase in appropriations through the annual budget process, if needed.

Judicial Department. To the extent that this bill increases the number of computer crime offenses prosecuted, workload for the trial courts will increase. Given that a Judicial Officer can handle 511 cases per year and the increase in cases resulting from this bill is expected to be well below this level, no additional appropriations are required.

State agencies. State agency workload increases to review record disposal policies to ensure such policies are in compliance with this bill. To the extent that encryption, redaction, or other means are needed to ensure these records are unreadable costs may increase. This analysis assumes additional appropriations will be requested through the annual budget process, if needed.

Centrally appropriated costs. Pursuant to a Joint Budget Committee policy, certain costs associated with this bill are addressed through the annual budget process and centrally appropriated in the Long Bill or supplemental appropriations bills, rather than in this bill. These costs, which include employee insurance and supplemental employee retirement payments, are estimated to be \$2,470 in FY 2018-19 and \$3,668 in FY 2019-20.

Local Government

Overall, this bill is expected to increase local government revenue, costs, and workload as described below. The exact impact to a particular local government will vary depending on existing record disposal policies and the number of new computer crime offenses committed within its jurisdiction.

Record disposal policies. Beginning in FY 2018-19, this bill increases local government workload to update record disposal policies. To the extent that encryption, redaction, or other means are needed to ensure these records are unreadable, costs may increase. These potential costs have not been estimated.

District attorneys. The bill may increase workload and costs for district attorneys to prosecute any new offenses misdemeanor computer crime offenses, discovered from the new reporting requirements created by this bill.

County jails. Under current law, a court may sentence an offender to jail for a misdemeanor or petty offense computer crime. The sentence period varies depending on the nature of the offense and can be up to 18 months. Because the courts have the discretion of incarceration or imposing a fine, the precise impact at the local level cannot be determined. Estimated costs to house an offender in a county jail vary from \$53 to \$114 per day. For the current fiscal year, the state reimburses county jails at a daily rate of \$54.39 to house state inmates.

Denver County Court. The bill may increase criminal fine and court fee revenue, costs, and workload for the Denver County Court, managed and funded by the City and County of Denver from any new misdemeanor computer crime cases. Probation services in the Denver County Courts may also experience a minimal increase in revenue and workload to supervise persons convicted under the bill within Denver County.

Effective Date

The bill takes effect September 1, 2018.

State Appropriations

For FY2018-19, this bill requires a General Fund appropriation of \$9,157 and an allocation of 0.2 FTE to the Department of Personnel and Administration.

State and Local Government Contacts

All Local Agencies

All State Agencies