

ANALYSIS OF AMENDED BILL

Author: Waldron Analyst: Janet Jennings Bill Number: AB 322
 Related Bills: None Telephone: 845-3495 Amended Date: March 26, 2015
 Attorney: Bruce Langston Sponsor _____

SUBJECT:	Privacy/Social Security Numbers
-----------------	---------------------------------

SUMMARY

This bill would require a person, entity, state agency, or local agency to encrypt social security numbers (SSN), as specified.

This analysis only addresses the provisions of this bill that impact the department’s programs and operations.

RECOMMENDATION

No position.

Summary of Amendments

The March 26, 2015, amendments removed provisions of the bill related to the Health Insurance Portability and Accountability Implementation Act, and replaced them with the provisions discussed in this analysis. This is the department’s first analysis of the bill.

REASON FOR THE BILL

The reason for the bill is to protect social security numbers from being disclosed.

EFFECTIVE/OPERATIVE DATE

This bill would become effective on January 1, 2016, and specifically becomes operative on July 1, 2017.

FEDERAL/STATE LAW

Current federal and state tax laws require that an individual's SSN be used as the identifying number for that individual with regard to income taxes. Current state tax law provides that information collected on income tax returns is considered confidential and, unless specifically available for other uses, must be used only to administer the income tax laws. The Franchise Tax Board (FTB) may disclose taxpayer information only in limited circumstances and only to specific agencies as authorized by law. Improper disclosure of federal tax information is punishable as a felony, and improper disclosure of state tax information is punishable as a misdemeanor.

Board Position:	Executive Officer	Date									
<table style="width: 100%; border: none;"> <tr> <td style="width: 33%;"><u> </u> S</td> <td style="width: 33%;"><u> </u> NA</td> <td style="width: 33%;"><u> </u> X NP</td> </tr> <tr> <td><u> </u> SA</td> <td><u> </u> O</td> <td><u> </u> NAR</td> </tr> <tr> <td><u> </u> N</td> <td><u> </u> OUA</td> <td><u> </u></td> </tr> </table>	<u> </u> S	<u> </u> NA	<u> </u> X NP	<u> </u> SA	<u> </u> O	<u> </u> NAR	<u> </u> N	<u> </u> OUA	<u> </u>	Selvi Stanislaus	05/19/15
<u> </u> S	<u> </u> NA	<u> </u> X NP									
<u> </u> SA	<u> </u> O	<u> </u> NAR									
<u> </u> N	<u> </u> OUA	<u> </u>									

Under the Information Practices Act of 1977, current state law requires state and local agencies to maintain in their records only that personal information relevant and necessary to their governmental purposes, including disclosing personal information under only specific circumstances and keeping records thereof. "Personal information" is defined as any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, SSN, physical description, home address, home telephone number, education, financial matters, and medical or employment history. The definition also includes statements made by, or attributed to, the individual. The Information Practices Act establishes civil remedies for the enforcement of its provisions.

PROGRAM BACKGROUND

Under current department practice, the department collects personal information from various sources, including from the taxpayer and from agencies required to report financial information. This information is used for compliance development, audit, and collection purposes. The FTB does not use personal information or provide that information to third parties for any marketing purposes. As required by statute, all information received from the taxpayer is confidential and is shared with federal or state agencies only for statutorily specified purposes.

The FTB has stringent departmental policies and procedures regarding privacy and disclosure. All employees receive training annually about ensuring the confidentiality of taxpayer information and are given updated procedures on a regular basis. Any violation of these policies and procedures is subject to disciplinary action, punishable by law, or both.

The basic design of the FTB's personal income tax (PIT) mainframe computer system relies on using the SSN as the taxpayer's account number. The PIT system feeds information to other related systems, including collection and audit systems. All refunds, billings, and taxpayer communications relating to the taxpayer's account, including communications regarding audit and collection activities contain the taxpayer's SSN.

THIS BILL

This bill would require a state agency to encrypt a SSN if it is electronically collected, retained, maintained, licensed, or used. In addition, a state agency may not electronically share, transmit, or disclose a SSN unless the connection is secure or the SSN is encrypted.

The above requirements would be inapplicable if any of the following circumstances are met:

- The state agency alters the SSN or uses other security measures to ensure the SSN cannot be linked to a specific individual.
- The state agency is covered by contract or other legally enforceable prohibition with a third party that would prevent the third party from attempting to link the data to a specific individual.
- The SSN is used for public licenses, or public records associated with employment, when collected or used by an employer or third party for employment status.

- If the state agency collects, retains, maintains, licenses, uses, shares, transmits, or discloses fewer than ten thousand SSNs in a 12-month period or has five or fewer employees, and doesn't knowingly collect, retain, maintain, license, use, share, transmit, or disclose any information that includes personal data linked with SSNs.
- If the state agency is covered by one of several specifically identified federal privacy or security laws, including any other federal privacy law or regulation enacted after January 1, 2015. For a full list of specifically identified laws see Appendix A.

IMPLEMENTATION CONSIDERATIONS

The department has identified the following implementation concerns. Department staff is available to work with the author's office to resolve these and other concerns that may be identified.

This bill uses terms that are undefined, i.e., "encrypted," "electronically share," "connection is secure," "other security measures," "linked to a specific individual." The absence of definitions to clarify these terms could lead to disputes with taxpayers and would complicate the administration of this bill. The author may want to amend the bill to clearly define the terms.

The department receives data that includes SSNs from many sources including the IRS, banks and financial institutions, taxpayers, title companies, courts, and other state tax agencies. The bill lacks a provision to allow the use of SSNs for tax administration purposes, which is problematic for the department. In order to conduct the daily activities of the department, encryption keys would need to be set up for every party the department communicates with by fax or other electronic means. The author may wish to amend the bill to provide an exemption for tax administration purposes.

This bill would provide an exception for state agencies that are subject to any of a number of specified federal privacy and security laws. Yet the bill lacks exceptions for state agencies that are subject to (1) federal laws that prohibit the unauthorized disclosure of federal tax returns and returns information, or (2) state privacy and security laws. The author may wish to amend this bill to add these laws to the specified exceptions.

TECHNICAL CONSIDERATIONS

For accuracy, the author may wish to amend the bill language that reads "Any other privacy law or regulation enacted" to read, "Any other privacy law enacted or regulation adopted."

OTHER STATES' INFORMATION

Most states have privacy laws that are similar to California's privacy laws and the federal Privacy Act prohibiting various state and local agencies from disclosing personal identifying information, such as an SSN, in an unauthorized manner. Some states have additional laws relating to identity theft; however, they do not further restrict disclosure and use of personal identifying information by revenue collecting agencies.

FISCAL IMPACT

The cost to implement this bill cannot be determined until implementation concerns have been resolved. As the bill continues to move through the legislative process and the implementation concerns are resolved, costs will be identified and an appropriation will be requested, if necessary.

ECONOMIC IMPACT

This bill would not impact the state's income tax revenue.

SUPPORT/OPPOSITION

Support: None on file.

Opposition: None on file.

ARGUMENTS

Proponents: Some may argue this bill would provide individuals greater protection of their SSNs.

Opponents: Some may argue this bill would increase the complexity of matching records to the appropriate individual due to SSNs being encrypted.

LEGISLATIVE STAFF CONTACT

Janet Jennings
Legislative Analyst, FTB
(916) 845-3495
janet.jennings@ftb.ca.gov

Jame Eiserman
Revenue Manager, FTB
(916) 845-7484
jame.eiserman@ftb.ca.gov

Gail Hall
Legislative Director, FTB
(916) 845-6333
gail.hall@ftb.ca.gov

Appendix A

The Privacy Act of 1974 (5 U.S.C. Sec. 552a).

The Right to Financial Privacy Act of 1978 (12 U.S.C. Sec. 3401 et seq.).

The Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

The Fair Debt Collection Practices Act (15 U.S.C. Sec. 1692 et seq.).

The Children's Online Privacy Protection Act of 1998 (15 U.S.C. Sec. 6501 et seq.).

Title V of the Gramm-Leach-Bliley Financial Modernization Act (15 U.S.C. Sec. 6801 et seq.).

Chapters 119, 121, 123, and 206 of Title 18 of the United States Code.

The Family Educational Rights and Privacy Act of 1974 (20 U.S.C. Sec. 1232g).

The Protection of Pupil Rights Amendment (20 U.S.C. Sec. 1232h).

Sections 5701 and 7332 of Title 38 of the United States Code.

The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d-2 et seq.).

The Privacy Protection Act of 1980 (42 U.S.C. Sec. 2000aa line 30 et seq.).

Part C of Title XI of the Social Security Act.

Subtitle D of Title IV of the Health Information Technology for Economic and Clinical Health Act, which was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5).

The E-Government Act of 2002 (44 U.S.C. Sec. 101 et seq.).

The Paperwork Reduction Act of 1995 (44 U.S.C. Sec. line 38 3501 et seq.).

Any other federal privacy law or regulation enacted after January 1, 2015.