OHIO LEGISLATIVE SERVICE COMMISSION

www.lsc.ohio.gov

Office of Research and Drafting

Legislative Budget Office

H.B. 376
134th General Assembly

Fiscal Note & Local Impact Statement

Click here for H.B. 376's Bill Analysis

Version: As Reported by House Government Oversight

Primary Sponsors: Reps. Carfagna and Hall

Local Impact Statement Procedure Required: No

Jessica Murphy, Budget Analyst

Highlights

- The bill establishes requirements for businesses related to the collection, processing, and sale of digital personal data. It appears that the scope of the bill mostly applies to large businesses with many exemptions.
- The Attorney General is provided with exclusive authority to enforce the requirements of the bill. The bill expressly states that it is not to be construed as authorizing a consumer to bring a lawsuit against a covered business, including a class action lawsuit, and provides affirmative defense against lawsuits brought under the bill.
- Staff of the Attorney General estimate their annual operating costs of enforcing the bill's requirements at about $556,000, with close to 70% paying for the payroll costs of three full-time staff (two attorneys and one analyst).

Detailed Analysis

The bill establishes requirements related to the collection, processing, and sale of digital "personal data"[1] that fall into two primary categories: (1) requirements imposed on companies that collect or process personal data and (2) rights provided to consumers whose personal data

[1] Under the bill, "personal data" means any information that is linked or reasonably linkable to an identified or identifiable consumer and that is processed by a business for a commercial purpose, excluding any such data processed from publicly available sources or pseudonymized, deidentified, or aggregate data.

is collected. The Attorney General is authorized as the sole entity to enforce the bill's requirements, which take effect one year after the bill's effective date.

Covered businesses

As it relates to businesses, the bill establishes requirements regarding the collection, processing, and sale of digital personal data, as well as requirements to comply with requests made in relation to consumer rights.[2] The requirements apply to a business that conducts business in Ohio, or whose products or services target consumers in Ohio, that meet any of the following criteria:

- Gross annual revenue exceeds $25 million;
- Controls or processes personal data of 100,000 or more consumers during a calendar year;
- During a calendar year, derives more than 50% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 or more consumers.

Under the bill, "consumer" encompasses only Ohio residents acting in an individual or household context and not individuals acting in a business capacity or employment context.

The bill targets businesses that warehouse very large volumes of personal data on consumers and potentially sell that data. The Ohio Small Business Association supports this assessment, indicating to the CyberOhio Advisory Board that a very small fraction of their membership would be affected by the bill.[3] It is difficult to determine how many businesses would fall within the scope of the bill, partially because of the bill's many exemptions. For example, the bill's requirements do not apply to certain businesses, industries, and data if they are already subject to federal data privacy standards such as through GLBA, HIPAA, FERPA, and FCRA.[4]

Data processors

The bill regulates the relationship between covered businesses and data processors in relation to personal data. Covered businesses are required to enter into a written contract with a processor that prohibits the processor from processing personal data except to provide services to the business. Processors are required to take specified actions regarding the contract.

[2] The bill provides basic rights to consumers with regard to their personal data: (1) a right to know what data is being collected about them, (2) a right to request that data, (3) a right to correct inaccuracies in that data, (4) a right to have their data deleted, and (5) a right to prohibit the sale of their data.

[3] The CyberOhio Advisory Board is under InnovateOhio.

[4] Gramm-Leach Bliley Act (GLBA) governs financial institutions' use and protection of nonpublic personal information; Health Insurance Portability and Accountability Act (HIPAA) protects certain health information and generally applies to three covered entities including most health care provides; Family Educational Rights and Privacy Act (FERPA) protects the privacy of students' education records; Fair Credit Reporting Act (FCRA) governs the acts of credit reporting agencies (CRAs), entities that furnish information to CRAs (furnishers), and individuals who use credit reports issued by CRAs.

Enforcement

As noted, the bill establishes the Attorney General as the sole entity to enforce the bill's requirements. The bill expressly states that it is not to be construed as authorizing a consumer to bring a lawsuit against a covered business or processors, including a class action lawsuit.

According to staff of the Attorney General's Office, there are several provisions of the bill that affect staffing. A considerable amount of time and effort will likely be required to determine whether a business is subject to the bill. The Attorney General anticipates the determination process to work similar to an audit. This type of review requires the opinion of an attorney, as well as an analyst with specialized technical training.

Staff of the Attorney General estimate their annual operating costs of enforcing the bill's requirements at about $556,000, with close to 70% paying for the payroll costs of three full-time staff (two attorneys and one analyst). Apparently, the salaries for attorneys in the data privacy field can be relatively high due to demand for their specialized skills.

The bill authorizes the Attorney General to use $250,000 of GRF line item 055321, Operating Expenses, in FY 2023 for enforcement costs. These annual amounts are around $300,000 less than the Attorney General's estimated cost of $556,000. Because of the nature of the Attorney General's operating budget, this relatively small funding shortfall may not be problematic. The Attorney General's total appropriated operating budget for FY 2023 is $398.3 million. The FY 2023 appropriation for GRF line item 055321 totals $71.6 million; there is no law restricting the Attorney General from allocating more than the above-noted $250,000 from that line item to enforce the bill's requirements. The Attorney General also has access to two unrestricted non-GRF funds that may carry cash balances sufficient to make up any operating cost shortfall: the General Reimbursement Fund (Fund 1060) and the Attorney General Claims Fund (Fund 4190).

The bill provides a path to compliance without legal enforcement through a 30-day cure period for any business found in violation. The type of relief that can be sought by the Attorney General filing a civil action in a court of common pleas includes a declaratory judgement, injunctive relief, civil penalties of up to $5,000 for each violation, attorneys' fees and investigative costs, and other court-ordered (consumer) relief.[5] All money awarded, except for consumer relief, is deposited into the Attorney General's existing Consumer Protection Fund (Fund 6310).

If the Attorney General has reasonable cause to believe that a covered business has engaged or is engaging in an act or practice that violates the bill's requirements, the Attorney General may initiate a lawsuit and seek civil penalties of up to $5,000 for each violation. Appropriate relief may be awarded to each identified consumer affected by a violation of the bill's requirements, regardless of whether any actual damages were suffered. As mentioned, prior to initiating any such lawsuit the Attorney General is required to provide a 30-day cure

[5] Court-ordered consumer relief for each consumer is $100 to $750 per violation regardless of whether any actual damages were suffered. If the court finds that the violation was willful or made knowingly, the court may triple the award.

period. This may reduce the frequency with which the Attorney General files a civil action and takes a matter to trial.

Affirmative defense

The bill provides an affirmative defense against lawsuits brought under the bill, similar to that set forth in Ohio's Cybersecurity Safe Harbor Law.[6] However, in order to assert the defense, the covered business must satisfy all components of a three-prong test. First, the covered business must establish a privacy program that meets a national standard. Second, that program must be kept up to date, mirroring the national standard. And third, the covered business's privacy program must be appropriate given the business's size and nature. The affirmative defense may prevent, to some degree, court actions that might have otherwise been initiated against a business after the 30-day cure period.

Anecdotal evidence suggests that large businesses, to which the bill will predominately apply, typically have privacy plans in place, although not all are uniform and may be limited in scope. The bill's affirmative defense includes adopting a privacy program that reasonably conforms to the National Institute of Standards and Technology (NIST) Framework that is widely considered the gold star of privacy protection.

HB0376HR/lb

[6] S.B. 220 of the 132nd General Assembly.