House Government Oversight Committee
Proponent Party Testimony
House Bill 376
John Virden, Assistant Vice President for Security, Compliance, and Risk Management and Chief Information Security Officer, Miami University
October 28, 2021

Chairman Wilkin, Vice Chair White and Ranking Member Hicks-Hudson, thank you for the opportunity to testify today on House Bill 376. My name is John Virden, I am the Assistant Vice President for Security, Compliance, and Risk Management and Chief Information Security Officer at Miami University. I am providing proponent party testimony on the bill.

House Bill 376 seeks to improve the protection of Ohio consumer's fundamental rights and clarify what covered businesses that process personal data must do to safeguard these rights. All covered businesses and organizations that deal with data related to Ohio consumers must comply. Thus, the bill will contribute to the accomplishment of an area of freedom, security and justice, to economic and social progress, to the strengthening of the Ohio economy, and to the well-being of consumers.

This legislation can act as a stimulus for broader change and can create new business opportunities. The implementation of privacy best practices within businesses is not just a quick fix, and with new processes in place and more robust data platforms, organizations will be better able to mine their data and decades of experience. Some forward-looking businesses will work on implementing this act alongside wider digital transformation projects across websites and applications that reinvent their company, their brand, ways of doing business, and transacting with consumers.

The bill's recommendation for covered businesses to satisfy all components of the three-prong test puts in place the establishment of a privacy program following the National Institute of Standards and Technology (NIST) Privacy Framework, while ensuring program currency, and ensuring their program fits the business's size and nature.

I have had the opportunity to experience firsthand the attempted implementation of two very similar regulations, the General Data Protection Regulation (GDPR) of Europe and the California Consumer Privacy Act (CCPA), both while performing the role of Chief Information Security Officer at the University of California, Riverside. I would like to share some of the challenges or stumbling blocks based on my experience.

Ohio can be a leader of consumer privacy protection if it can master the following five areas.

First, Program Implementation. Compliance with the bill offers covered businesses an affirmative defense against allegations of violations of privacy chapters. A privacy program is no small undertaking. The bill expects reasonable conformance with the NIST Privacy Framework.

Implementation of the NIST framework requires some level of resourcing by the covered business, including:

- Persons to research, analyse, identify risk, and implement the program.
- Processes that are needed in place to govern the program, currency reviews, control practices, and communication for consumers. Needed processes also include incident response, recovery plans, and business continuity.
- And potentially some level of technology to manage configurations, data backups, restorations, and vulnerability management.

All parties need to be aware, to ensure successful implementation of a covered business's program will require additional guidance, training, awareness, and resource support to meet appropriate NIST compliance.

Second, Local Policy. The right of a consumer to know what personal data a company has collected about them should be explicitly covered and posted in a company privacy policy. Privacy policy content requirements are very encompassing and comprehensive.

A covered business may need consultation, guidance, or templates to successfully instantiate a compliant policy document. Creating opportunities to share best practices and guidance should be considered, as well as, an industry practice of continuous review, updating, and maintenance of privacy policies as business functions, processes, needs, and goals change.

Third, Technology Challenges. The rights to access or delete a consumer's personal data, through a verifiable request, are provided in this bill. Appropriate exemptions for deletions are also available should the business need to maintain the consumer's personal data to comply with regulations, investigations, and other business or lawful bases.

Accessing or deleting personal, or any, data, can present process and technical challenges.

The deletion of personal data from all records held by a covered business can present challenges to complete, even within the allotted 45 days to either delete a consumer's personal data or notify the consumer of its refusal to make such a deletion. An unspecified time allowance is stated in the bill permitting a delay in compliance with a consumer's request to delete until the archived or backup system relating to that data is restored to an active system, next accessed, or used for a sale, disclosure, or commercial purpose.

The ability to delete specific data fields or records is not built into a number of tools and systems today. This may present difficulties for some covered businesses to fulfill consumer requests for deletion of personal data.

Even with the delay allowance for deletion of archived or backed up data, it can be challenging to locate all the data instances. For example, a system may backup data on a magnetic tape medium and perhaps to a cloud backup solution. Often, we routinely recommend organizations

maintain a number of backup locations including both onsite and offsite for redundancy. Additionally, it is not uncommon for these backup solutions to maintain many copies of backup data, sometimes even a month's worth of daily backups. A process and technology would need to be in place to find all data instances and delete each one, all while maintaining integrity of the non-deleted data fields.

An allowance is made in the bill for delayed deleting of personal data until the next restoration or when next accessed. Current practices of many organizations and institutions may not routinely conduct data restorations or routinely access archived data.

Success for our covered businesses in meeting bill compliance demands businesses be provided the guidance necessary to develop clear processes and implement appropriate technologies to feasibly achieve deletion requests that do not fall into the exemption categories.

Fourth, The personal data behind the scenes. The bill defines personal data "any information that relates to an identified or identifiable consumer processed by a business for a commercial purpose." This typically encompasses data types such as social security numbers, driver's license numbers, state identification cards, account or credit card numbers, and associated security codes. Other lesser known personal data may exist in the form of internet protocol (IP) addresses, device identifiers, and network transactional information including system logins, application accesses, and authentication records. These data types can be identifying information pointing to specific persons.

Lawful investigations can rely on detailed and complete data to provide a factual basis for legal cases. Should some of that data be deleted due to consumer request, legal judgement may be impaired. System performance maintenance and troubleshooting relies on network and system transactional data that may contain personally identifiable information. The removal of those data types could hamper system troubleshooting, potentially degrading or damaging system performance and business objectives.

To best ensure covered businesses have a thorough understanding of what constitutes personal data and to clarify if electronic device identifiers and network transactional data should be included, detailed guides and examples should be available for review.

Fifth, Retention conflicts. A business, or an associated processor, shall not be required to comply with a consumer's request to delete personal data if it is necessary for the business or service provider to maintain the consumer's personal data in order to adhere to its written records retention schedule.

This exception may be open to misuse when combined with the right to delete personal data. This intersection may be worth examining. For example, upon a consumer's request a business must delete the personal data or notify of reason of refusal. However if the business's retention policy states that particular personal data (PII, financial, health, etc.) must be retained for five years, then a conflict exists.

Alleviating confusion or misinterpretation on the part of the consumer requires that the covered business be very up front about company data retention policies. The posted privacy policy should include these details as clearly as possible.

In conclusion, HB 376 is needed and can be of great positive impact. Too often process and technical implementation challenges prove to be roadblocks to successful achievement to consumer privacy. When challenges such as these exist without guidance, training and technical solutions, compliance rarely occurs. Often the easier route is taken, but we can challenge ourselves to do what is difficult. I recommend consideration for supplemental guidance and resourcing to aid Ohio business success and ultimately consumer privacy goals.

Thank you for your time today, I am happy to answer any questions you may have.
