Introduction

Despite persistent **bipartisan calls** for data privacy protection, Washington has failed to enact federal data privacy legislation, leaving states to address ongoing data privacy **concerns** for themselves. Accordingly, Ohio lawmakers have introduced the **Ohio Personal Privacy Act** (House Bill 376). This admirable legislation fills Washington's void better than most data privacy rules thus far. Its scope is narrowly tailored and designed to reduce foreseeable costs on businesses and consumers, it prudently attempts to balance the privacy and economic interests of Ohio, and it tries to limit the reach and likelihood of unintended consequences suffered by other jurisdictions. The legislation is not perfect and improvements can be made, but the Ohio Personal Privacy Act takes a solid step in the right direction.

Reducing Foreseeable Costs of Data Privacy Protection

State-level data privacy legislation imposes costs and burdens on consumers and businesses, including the costs of market concentration, market **uncertainty**, and a range of **compliance requirements**. The Ohio Personal Privacy Act adopts a series of backstops to keep these costs in check and stay the heavy hand of bureaucratic regulation, but some burdens will persist.

Data privacy regulation **imposes** disproportionate costs on small and emerging businesses, for example, that can lead to market concentration among larger firms. An impact assessment of California's restrictive data privacy law **found** that smaller businesses were "likely to face a disproportionately higher share of compliance costs relative to larger enterprises." Those disproportionate compliance costs foster market concentration and create another advantage for larger firms.

The Ohio Personal Privacy Act takes several other steps to narrow its focus and reduce the costs it imposes on businesses. Like legislation in other states, Ohio's bill includes minimum-revenue and minimum-customer triggers that will limit—but not eliminate—costs for Ohio's small businesses. The legislation includes a 30-day "cure period" for regulated firms to remedy alleged violations before facing enforcement action; offers a unique "affirmative defense" for businesses that follow the National Institute of Standards and Technology data protection rules; and it exempts from regulation consumers acting in a business capacity. Accordingly, the CyberOhio Advisory Board has **indicated** that only a "very small fraction of their membership would be affected by the bill."

Even this carefully crafted law, however, will impose significant costs. California, for instance, estimated that its initial round of data privacy legislation would cost $55 billion—nearly 1.8 percent of its **gross state product**—and impact 50 to 75 percent of California businesses. Although less restrictive than the California law, the Information Technology & Innovation Foundation **estimates** that Ohio's data privacy law will cost $4.2 billion annually for "in-state"

costs alone—in addition to the costs incurred by the nightmarish web of other data privacy laws being implemented in other states. Add to these the cost of **hiring** lawyers and software engineers to ensure regulatory compliance, the $1,400 **price tag** for a single access data request, and the **hidden economic cost** of stunted investment and start-up activity, and Ohio's legislation may cost more than many currently anticipate.

Limiting Unintended Consequences

Perhaps even more worrying than projected financial costs, however, may be the unintended consequences imposed by data privacy bills. So-called "Right to Delete" provisions in Ohio's bill, for example, will make notifying consumers of **product recalls** more difficult. Data **privacy laws** also have been known to **stall research**, such as cancer studies, and make mundane tasks—like **grocery stores** helping the elderly—more difficult. Europe's data privacy law even **enabled** a hacker to access online accounts of a technology executive and steal her home address, credit card information, and music history.

The Ohio Personal Privacy Act addresses some concerns over hacking and data breaches, for example, by not requiring any business to "collect personal data that it would not otherwise collect in the ordinary course of its business," and by allowing companies to redact certain personal information in their responses to consumers. These antidotes are not perfect and they, too, come at a cost. Failing to collect some personal information from customers could create other compliance issues and court battles. And protecting consumer data and privacy may mean that businesses omit important information in their correspondence. Ohio's legislation may not be perfect and not every unintended consequence can be anticipated and averted, but the bill balances the foreseeable tradeoffs better than many other data privacy regimes.

Conclusion

The Ohio Personal Privacy Act would be **among the best** data privacy laws enacted or being considered. The bill is carefully tailored to limit its scope and reduce foreseeable financial costs and burdens on businesses and consumers. But policymakers should be aware that the regulatory price may prove higher than anticipated, and the hidden pitfalls of unintended consequences remain. As Ohio continues to balance the need for data privacy protection and the costs and risks of providing it, lawmakers should continue to seek ways to harmonize Ohio's data privacy rules with those enacted in other states.