Interested Party Testimony and Statement for the Record
Josh Harris
Director, Global Privacy Initiatives, BBB National Programs

Interoperability and H.B. 376, Ohio Personal Privacy Act (OPPA)
Ohio House of Representatives
Government Oversight Committee

December 8th, 2021

Chairman Wilkin, Vice Chair White, Ranking Member, Brown and members of the House Government Oversight Committee, thank you for the opportunity to testify today on House Bill 376, the Ohio Personal Privacy Act (OPPA). My name is Josh Harris, Director of Global Privacy Initiatives at BBB National Programs, a non-profit organization where businesses go to enhance consumer trust, and where consumers are heard.

At BBB National Programs, companies, industry experts, and trade associations work together to foster industry best practices in consumer dispute resolution, truth-in-advertising, child-directed marketing, and – most relevant to today's discussion – data privacy. Our Global Privacy Division operates certification and dispute resolution services built upon key elements of several government-backed privacy frameworks. These co-regulatory frameworks were designed and endorsed by participating governments to bridge gaps between divergent privacy and data protection regimes. By using our independent accountability mechanisms, participating businesses strengthen standards for data privacy and enhance consumer trust in the digital marketplace.

As the number of U.S. states and foreign countries developing privacy regulations continues to grow, so too has the importance of finding practical mechanisms to ensure these laws can mesh in a way that protects consumers while promoting compliance efficiency. To that end, we are pleased to see the commonalities the proposed OPPA bill has with other state laws and hope this marks an emerging consensus on a set of baseline privacy practices. It is also important that such best practices be leveraged as a safe harbor, as OPPA does in section 1355.09.

In our experience, safe harbors not only encourage the spread of best practices, but they also provide a key mechanism to advance privacy interoperability between states and nations alike. Operationalized safe harbors, including those pursuant to third-party accountability reviews, can help establish 'rules of the road' for businesses to implement practical compliance methodologies, assist enforcement authorities in assuring those methodologies are maintained, and enhance consumer understanding of what a business's OPPA-compliance means for them.

This approach is embodied in one of the United States' primary international commercial privacy initiatives: the OPPA-compatible Cross Border Privacy Rules (CBPR) certification system, whose role in promoting digital trade and consumer protection I highlight today. The CBPR

certification standards were developed by the United States Department of Commerce along with their counterpart Departments and Ministries participating in the Asia Pacific Economic Cooperation (APEC) Forum in 2007. Since that time, CBPRs have been recognized as a critical tool for interoperability across a range of trade agreements and laws, including in:

- The U.S-Mexico-Canada Agreement (USMCA): Among the major updates in the USMCA is the inclusion of a digital trade chapter. Article 19.8 (6) specifically recognizes the CBPR system as "a valid mechanism to facilitate cross-border information transfers while protecting personal information." This recognition ensures that participating companies can continue to use CBPRs as a transfer mechanism as privacy laws develop in the three signatory countries in the years ahead.
- The US-Japan Digital Trade Agreement: Paralleling the structure of the USMCA's digital chapter, this update to the US-Japan Free Trade Agreement promotes "the interoperability of enforcement regimes, such as the APEC Cross-Border Privacy Rules system (CBPR)." Inclusion of the CBPR system as a safe harbor under section 1355.09 can serve to encourage OPPA-compliant best practices while promoting increased digital trade and investment in Ohio from those jurisdictions such as Japan that recognize the CBPR certification.
- Japan's Act on the Protection of Personal Information (APPI): Article 24 of the Amended APPI provides that personal data may be transferred to a third party in a foreign country in the same way as an in-country transfer in cases where the recipient or provider has obtained the APEC Cross Border Privacy Rules (CBPR) certification.
- Singapore's Personal Data Protection Act (PDPA): The Government of Singapore's Infocomm Media Development Authority (IMDA) specifically recognizes CBPR certifications for overseas transfers of personal data under the PDPA.

To date, a total of 9 countries have joined the system and are working on how they too might recognize a CBPR certification under their privacy laws. Through the International Trade Administration, the United States Department of Commerce is also leading efforts to expand CBPR participation beyond the Asia-Pacific region so that it might eventually serve as a global compliance mechanism.

Most critically, CBPRs meet the business obligations under OPPA as found in sections 1355.03, 1355.04, 1355.05. 1355.06 and 1355.08, respectively. I note that United States is also a participant in the Privacy Recognition for Processors (PRP) certification program, a companion program to the CBPR system that certifies data processors. Recognition of PRPs may be particularly useful in the context of section 1355.08.

I want to stress, however, that we do not believe such certifications should be mandatory, nor exclusive. In fact, inclusion of the International Trade Administration-led CBPR and/or PRP systems as voluntary options for those businesses that so chose to participate complements OPPA's recognition of a written privacy program that reasonably conforms to the National Institute of Standards and Technology's (NIST) privacy framework in section 1355.09 (I)(1)(a).

While NIST and International Trade Administration work within the Department of Commerce on different aspects of data privacy, their work should be understood as complementary, with one as a technical guidance document and the other as certification system in service of international trade. Given both the technical and economic implications of data privacy and data flows, it is necessary to engage with the work of both sister agencies in OPPA in much the same way. Recognition of the CBPR certification system would afford more compliance options for Ohio businesses of all sizes and with differing use cases, while ensuring their baseline obligations under OPPA are being met.

Finally, similar compatibility can be found between the CBPR system and the business obligations under the Virginia Consumer Data Protection Act (VCDPA) as well as under the Colorado Privacy Act (CPA). Looking forward, OPPA recognition of CBPR certifications under section 1355.09 could form the basis of future interstate cooperation on cross recognition in much the same manner as these certifications are being used in the international context thereby positioning Ohio for a leadership role in broader collaboration among states and key trading partners alike.

Thank you again for the opportunity to provide this testimony on behalf of BBB National Programs, and I am happy to answer any questions