ACT | GLOBAL APP ECONOMY CONFERENCE

APP STORE AGE VERIFICATION MANDATES

THE ISSUE:

The adult content industry and certain social media platforms are attempting to offload their responsibility to verify the ages of their users. These stakeholders are trying to sell lawmakers on an alternative regime that **shifts liability and compliance burdens onto *small business app developers* instead of social media and adult content websites.** The legislation introduced last Congress, the App Store Accountability Act (S. 5364 / HR 10364, 118th), roughly tracks similar state proposals and **would expose small business app companies to untenable new liability risks and compliance costs.**

WHY IT MATTERS TO SMALL BUSINESSES IN THE APP ECONOMY:

Bills like S. 5364 / HR 10364 would impose unnecessary new mandates and sources of liability on small business app companies that are rightfully the responsibility of social media platforms and adult content websites by:

- Requiring every app, regardless of size or purpose, to **create new systems to receive and verify flags from app stores indicating age category of every single user;**
- Requiring small business developers who are developing general audience apps to **create new systems to receive and verify parental consent for minor users before "allowing use of the app,"** even if the app has no relevance to children;
- Requiring small business developers to provide "readily available features for a parent to implement time restrictions with respect to the app of such developer;" and
- Imposing **mandates on providers of child-directed apps that likely conflict with existing child privacy laws** including the Children's Online Privacy Protection Act (COPPA).

WHAT'S ALREADY AVAILABLE FOR PARENTS AND DEVELOPERS:

Major app platforms provide extensive, granular, and ever-improving tools for both parents and developers. For parents, these tools allow for access and control of every application, including web browsers. They also allow parents to control amount of time their children have access to apps, control video and text messaging permissions, and access to something as simple as contact lists to prevent unauthorized people from reaching a child. Beyond privacy, parents control every single time children want to make a purchase, including in-app purchases. Moreover, they can control all of this remotely.

For developers, platforms provide a robust reporting mechanism for our members to identify applications that are directed at children and highlight features that might benefit both parent and child. Additionally, third-party tools exist for developers to receive verifiable parental consent if they intend to provide content for children under the age of 13. The rapid deployment of these features has come at the behest of parents, rather than by government mandate.

WHAT POLICYMAKERS CAN DO:

Oppose legislation like the App Store Accountability Act because it is a blatant attempt to distribute the responsibilities of providers of age-sensitive materials onto the rest of the ecosystem. This legislation would impose substantial, **unnecessary costs and liabilities on small business developers**, while letting social media platforms and adult content providers that are the source of the problem off the hook. **Perhaps worst of all, the bill also puts parents last, requiring that they accept parental control tools at the speed and flexibility of government.**

ACT | GLOBAL APP ECONOMY CONFERENCE

WHAT INNOVATIVE SMALL BUSINESSES NEED IN A PRIVACY BILL

THE ISSUE:

The United States lacks a federal data privacy law. Unlike many countries and jurisdictions around the world, the United States does not have a nationwide statute providing rules of the road for how companies should handle consumer data. Instead, American companies must operate in an environment with several sectoral laws governing certain types of data (health, banking, etc.) with large gaps in between. Worse, those gaps are increasingly being filled by conflicting state laws, creating a complex patchwork that gets more difficult to navigate by the year.

WHY IT MATTERS TO SMALL BUSINESSES:

Small businesses need a federal data privacy law. Small software and connected device companies like ACT | The App Association members handle millions of terabytes of data per day, putting them on the front lines of protecting and enabling responsible use of data. In fact, a competitive dynamic has developed among our members to meet customer expectations regarding privacy. However, without a federal comprehensive privacy law, businesses of every size are stuck in limbo caused by the failure of Congress to act. And unlike the biggest companies, small businesses do not have large, expensive compliance departments that can handle the ever-growing patchwork of state and international privacy laws.

WHAT POLICYMAKERS CAN DO:

Support a federal data privacy law that includes the "4 Ps of Privacy:" Preemption, no Private right of action, a Path to compliance, and Protection against unauthorized access. If Congress strikes the right balance on these concepts, it can help small businesses avoid the impending compliance tsunami from differing state laws and better enable our members to continue innovating, creating jobs, and revolutionizing industries.

1. **Preemption**
   New privacy legislation in Congress should establish a single, national set of requirements by preempting state privacy laws of general applicability that would create the most significant confusion, conflict, and compliance issues we have urged Congress to avoid. Lawmakers must avoid adding exceptions to preemption provisions causing courts to uphold state laws that differ substantially from federal requirements. Each exception to the preemption language adds further uncertainty, moving away from a single set of rules and back toward a divergent state patchwork.

2. Protection Against Unauthorized Access

Although most general privacy bills deal primarily with requirements surrounding consumer notice and consent for certain processing activities, we believe they should also require covered companies to take certain steps to detect, prevent, and remediate unauthorized access to personal information. These requirements should also preempt most state laws that would otherwise impose conflicting or substantially different data security obligations. Strong federal data security provisions would raise the average readiness of American companies to defend against cyberthreats of all kinds, from state-sponsored ransomware campaigns to social engineering and phishing attacks.

3. Path to Compliance

Requirements in any privacy law should be calibrated to the underlying risk of the processing activities in question and should allow small companies to demonstrate privacy competence without being subject to immediate civil penalties for even small violations. Going forward, privacy legislation should provide a path to ensure that smaller companies are rightfully viewed as—and held accountable for—complying with a federal framework, while alleviating liability concerns and compliance burdens that the bigger companies can more easily shoulder. One way to ensure coverage while not overburdening small businesses is a "compliance program" presumptively deeming businesses that certify adherence to industry-specific guidelines to be in compliance with the law.

4. No Private Right of Action

While there is a time and place for civil litigation, in the case of privacy laws, it often becomes a tool for abuse by opportunistic litigators rather than empowering consumers. Therefore, federal legislation should exclude a private right of action (PRA) and rely on existing legal authorities and agencies like the Federal Trade Commission (FTC). If an overly broad PRA is put into place, many businesses may be forced to settle meritless claims or divert limited resources away from hiring, research and development.