Global AppCon'22
Competition and Privacy
ACT | The App Association

Protecting Consumer Privacy Grows Small Business

Small businesses are both the key to a federal privacy framework and the leaders in developing privacy practices that work for consumers. While big businesses dominate the headlines, ACT | The App Association members handle millions of terabytes of data per day, putting them on the front lines of protecting and enabling good use of data. The App Association gives small, innovative companies a voice in the privacy debate in Congress and at federal agencies by illustrating how proposed laws and regulations will impact their ability to create jobs in your states and districts.

Trust is paramount for our member companies' success and when it comes to software, security and privacy are the cornerstones of trust. Our members know that consumers have important questions for companies that use and share their data. What data is being used or shared? Who is sharing data and with whom? How are they sharing or using it? The answer to these questions affects how consumers engage with the products and services created by our members.

To that end, we developed tools and guides to help our members comply with—and consumers understand—the Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), the California Consumer Privacy Act (CCPA), and the EU's General Data Protection Regulation (GDPR). Similarly, we conducted key user testing, including for the short-form privacy notice best practices developed through the National Telecommunications and Information Administration's (NTIA's) multistakeholder process in 2013.

The App Association recognizes that the modern notice and consent model is not always a sufficient means of communicating privacy expectations or establishing a relationship of trust. Consent often fails to contemplate dynamic uses of data and does not encapsulate consumers' future expectations given the passage of time or changing contexts. Now is the time for our industry, regulators, and policymakers to have a frank discussion on a federal privacy framework centered on consumer experience while preserving the ability for small innovators to compete and develop better privacy practices and communication methods.

Policymakers Should Keep the Following Considerations in Mind when Crafting Any Changes to Federal Privacy Law

- **A Single, National Standard.** New privacy legislation in Congress should establish a single, national standard. Our member companies may include the smallest software and connected device companies, but they serve customers across the nation and around the world. Complying with a patchwork of state laws would be unnecessarily burdensome because any single state's borders rarely coincide with the geographic footprint of an app maker's business. If privacy legislation does include a preemption provision, we would support limited rulemaking authority; allowing state attorneys general to enforce the bill's provisions; and a limited private right of action with appropriate guardrails to deter and prevent sue-and-settle business models that prey on small businesses.

- **Transparency , Access, and Control.** Federal privacy requirements should ensure businesses are transparent and allow users a reasonable level of control over the collection and use of information about them. For example, Colorado, Virginia, Utah, and Connecticut recently enacted laws that require companies to honor all or some of the following consumer rights: the right to access data about themselves; the right to correct inaccuracies; the right to delete such data; the right to opt out of certain processing activities including the sale of such data; and the right to port certain data about themselves to another service. Most importantly, all of these requirements must be implemented in a way that avoids additional compliance layers without enhancing consumer understanding and trust. App Association members compete on privacy and work hard every day to develop better ways to communicate with their users about privacy and give them meaningful choices. Consumers should have a clear understanding of the types of personal data they are sharing, and which companies are using that data and how.

- **Accountability.** The Federal Trade Commission (FTC) has long advocated for companies to incorporate privacy into the design and functionality of products and services. If privacy is a functional feature of a product or service, the protections, notices, and options it provides may shift and take on different forms depending on the context. Federal law should support the dynamic functionality of privacy by design by making companies accountable for sound privacy practices while allowing them to innovate on the details of their privacy programs.

- **Data Security.** Privacy legislation should also include a mandate for companies to take measures to secure data against unauthorized access or acquisition. Among other things, such a provision should require that data security policies and practices be appropriate to the size and complexity of a covered entity, the nature and scope of processing activities, and the volume and nature of data at issue. Protecting data against the risks of unauthorized access involves a set of activities that are different from protecting the privacy of consumer data and meeting consumer privacy expectations. Federal legislation should address both.

Oppose Policies that Prohibit Privacy Measures

Just as we urge policymakers to impose privacy and data security requirements on covered entities, we also oppose legislation that would create a presumption that platform-level privacy controls are illegal. For example, the American Innovation and Choice Online Act's (S. 2992's / H.R. 3816's) prohibition on a platform restricting access by app makers to personal information presumes that certain platform-level privacy and security controls are illegal. For example, the major mobile app stores currently prohibit app makers from requesting data that is irrelevant to the core functionality of an app. App stores enforce these data minimization requirements by removing apps that fail to adhere to the guideline, including Trojan horse apps and malware. By prohibiting the removal of these apps from consumer devices, S. 2992/H.R. 3816 would eliminate some of the most fundamental privacy and security protections consumers benefit from now in the mobile ecosystem. We urge policymakers to reject proposals like S. 2992/ H.R. 3816 on the grounds that they would not only fail to impose privacy requirements, but they would also outlaw beneficial privacy features developed by the market.

ACT | The App Association

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org/ actonline.org