STATEMENT OF KATHERINE KUEHN

MEMBER, NATIONAL TECHNOLOGY SECURITY COALITION, BOARD OF DIRECTORS AND CHIEF INFORMATION SECURITY OFFICER-IN-RESIDENCE

U.S. HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON INNOVATION DATA, AND COMMERCE

HEARING ON
LEGISLATIVE SOLUTIONS TO PROTECT KIDS ONLINE AND ENSURE AMERICANS' DATA PRIVACY RIGHTS

WEDNESDAY, APRIL 17, 2024
10:00 AM

2123 RAYBURN HOUSE OFFICE BUILDING

The **National Technology Security Coalition (NTSC)** is a nonprofit, nonpartisan organization that serves as the preeminent advocacy voice for the Chief Information Security Officer (CISO) and senior security technology executives. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.

Chair McMorris Rodgers, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky, and members of the Committee, thank you for the opportunity to testify today on the American Privacy Rights Act of 2024, the APRA. My name is Katherine Kuehn, and I am a member of the National Technology Security Coalition board of directors and serve as the CISO-in-Residence.

Established in 2016, the National Technology Security Coalition is a nonprofit, nonpartisan organization that serves as the preeminent advocacy voice for chief information security officers (CISOs), chief privacy officers, and senior security technology executives.

For those of you unfamiliar with the chief information security officer role, the CISO is a senior technology risk executive who is responsible for information and data security, cyber security, and technology security, of an enterprise. These men and women are charged with protecting the enterprise from information security risk, be it from nation-states, cyber-criminals, hacktivists, or an unknowing employee committing a non-malicious violation of the organization's policy. The CISO is on the frontline of securing our nation's data, including individual's private information, and our nation's critical infrastructure.

I sit before the committee today with over 25 years of experience leading and advising cyber security, technology, and innovative AI (Artificial Intelligence) strategies and teams to help the public and private sectors achieve more informed risk decisions. I have strived in my career to maintain a comprehensive understanding of all facets of the cyber ecosystem, through acting in numerous capacities, both on the practitioner and operator side, including Advisor, Board of Director, Chief Trust Office, Chief Information Security Officers, Chief Revenue Officer, and Chief Executive Officer. My career as a risk executive started here in Washington, as an intern for U.S. Senator Tom Harkin (D-IA). One of my responsibilities was to create his first website, and was given a book, *HTML for Dummies*, to help build it. I remember when we launched the first page being so proud of our work, but also genuinely concerned about the security, wondering if there would be ways in the future to take the data we provided, people we highlighted on the site, and use it in negative ways. It was the first time I ever had a concern about the bright future, the still very new internet held the promise of achieving, and from it, my career in cyber was born. All these years later, now a mother of five, the digital revolution we have witnessed has been indeed bright, but still, as I look to the future my children will face, gives me pause for concern.

As a career Risk Executive, it is not a surprise that the complexity of consumer data privacy has brought us all here today. In a recent study, it was highlighted that **9 out of 10** Americans consider their online privacy to be an important issue with **85%** of global adults wanting to do more to protect their online privacy.

I reflect on a comment made by Vint Cerf, widely accepted as one of the "fathers" of the internet, and a mentor of mine, from 2013, that Privacy may be an anomaly. I remember disagreeing with that comment then, and now over ten years later, with the rapid acceleration of social media, data mining, and targeted influence campaigns, it is clear to me that privacy with respect to our data, cannot be an anomaly, and must be protected.

Today, American consumers and corporations navigate a complex landscape of state-specific privacy laws. These state laws, while pioneering, create a patchwork of disparate regulations that can be confusing for consumers and burdensome for businesses, particularly those operating across state lines. Over the past few years, 17 states have enacted privacy laws and regulations with another 18 states actively pursuing various pieces of legislation. While the intention of these laws is noble, the result is a wide variation of protections and a resulting compliance nightmare for national and international businesses trying to comply with all of them.

In the absence of a federal privacy law, the average consumer has little to no understanding of the protections the states offer, as **1 in 4** Americans are asked to agree to a privacy policy every day and the potential ramifications to their privacy may differ from state to state. In addition, there is a risk that states could compete by offering looser regulations to attract business investment, leading to a "race to the bottom" in terms of privacy standards. This introduces new areas of risk, especially with the rapid adoption of Generative AI both in the consumer and business space. States trying to offer more comprehensive consumer data privacy could end up being penalized for trying to do the right thing. While the state-level protections are noble in thought, inaction from the federal government has the potential to hurt both American consumers and businesses, and potentially the states themselves. Individuals and their data are not protected equally.

The American Privacy Rights Act of 2024 represents a significant step towards consolidating and enhancing consumer privacy protections in the United States. The APRA proposes a unified federal standard that aims to streamline privacy protections nationwide, thereby benefiting both consumers and businesses by providing clarity and consistency. While the states will still actively participate in consumer privacy and protections, the beginning work of approaching these protections at a federal level is heartening.

One of the most significant advantages of the APRA is the centralization of privacy standards. Under the current system, businesses must adapt to the varying requirements of different state laws, which can be inefficient and costly. This fragmentation not only affects businesses but also leaves gaps in protection for consumers, depending on their state of residence. With two-thirds of global consumers feel that tech companies have too much control over their data, a federal standard under the APRA would be a big step forward in ensuring that all American consumers receive the same level of privacy protection regardless of where they live. This uniformity helps simplify the legal framework for businesses, particularly small and medium-sized enterprises that might lack the resources to navigate multiple regulatory environments.

The APRA is designed to offer robust consumer protections that go beyond many state laws. Key provisions may include the right to access, correct, and delete personal data, similar to the rights provided under the General Data Protection Regulation (GDPR) in Europe. Additionally, the APRA would potentially introduce stricter consent requirements for data collection, ensuring that consumers have a more active role in the management of their personal information. This is particularly important in an era where data breaches and unauthorized data sharing have become frequent. By establishing these rights at a federal level, the APRA ensures that all consumers can expect and receive a consistent, high standard of privacy protection.

The APRA would prevent the "race to the bottom" scenario by setting a baseline level of protection that states cannot undercut. This is critical as we face a future with even more reliance on data we create and leverage in new ways with the introduction of Generative AI. In addition, with the same current and future lens, this baseline ensures that the fundamental rights of consumers are preserved across the nation and that privacy standards cannot be compromised for economic gain. As a risk professional and a mother, this baseline is a major step forward, in the right direction of ensuring Privacy is not an anomaly.

The National Technology Security Coalition supports the American Privacy Rights Act of 2024 as it marks a significant improvement in the landscape of consumer privacy protections in the United States. By replacing the existing patchwork of state laws with a cohesive federal standard, APRA promises to provide uniform, robust privacy rights to all Americans.

The APRA not only enhances consumer protections but also simplifies compliance for businesses, prevents a dilution of privacy standards, and strengthens the U.S. position in the global digital economy. Adopting the APRA would signify a major step forward in aligning the United States with global best practices for data privacy and securing the trust and confidence of American consumers.

Chair McMorris Rodgers, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky, as you continue to work to develop a federal privacy standard, please consider the National Technology Security Coalition a resource moving forward. Thank you for the opportunity to appear before you today.