To: Members of the House Committee on Energy and Commerce's Innovation, Data, and Commerce Subcommittee
From: National Taxpayers Union
Date: April 16, 2024
Subject: NTU's Views on April 17, 2024 Subcommittee Hearing

I. Introduction and Key Taxpayer Considerations

On behalf of the National Taxpayers Union (NTU), the nation's oldest taxpayer advocacy organization, we write to express our views on several measures slated for consideration before the House Committee on Energy and Commerce's Innovation, Data, and Commerce Subcommittee. NTU applauds the Committee for your continued efforts to advance legislation that will protect taxpayers' data privacy. As such, NTU urges caution as the legislative process proceeds on the American Privacy Rights Act, H.R. 7891, and H.R. 7890.

H.R. ____ - The American Privacy Rights Act (APRA)

Against the backdrop of a growing patchwork of state privacy laws, this bipartisan legislation by House Energy and Commerce Committee Chair Cathy McMorris-Rodgers (R-WA) and Senate Commerce Committee Chair Maria Cantwell (D-WA) seeks to harmonize privacy rules across boundaries.

While Congress works to pass a much-needed comprehensive privacy law, it also needs to ensure that such a framework does not create more problems than it solves. To that end, ideal privacy legislation should harmonize privacy rules across both state boundaries *and* different sectors. The proposed APRA is likely to succeed on the first count but fail on the second because of exemptions for existing sectoral federal laws.

A better approach would entail establishing the same legal standards for all industries while developing distinct rules and liabilities for different data types. For example, a consumer's music streaming preferences do not carry the same privacy risks as sensitive financial and medical data, and privacy law should create distinct rules accordingly. Congress should distinguish between non-sensitive and sensitive data — such as educational records and biometric data. The strictest privacy standard should apply to sensitive data used to deliver critical services like surgeries, while the least strict standard should apply to non-sensitive data used to provide non-critical services, like music streaming.

Nevertheless, even within the framework of the APRA, several amendments could improve the proposed legislation. First, the overly broad, expansive private right of action under §19 could easily lead to an array of frivolous lawsuits against all types of companies. The proposed law would benefit from narrower and more targeted rights of private action, if not eliminating private rights of action altogether.

Second, at a time when the Federal Trade Commission has increasingly sought to act beyond its statutory authority, U.S. lawmakers should be cautious about granting the Commission more powers. That is precisely what the newly proposed FTC Bureau for privacy enforcement — similar to the existing Bureau of Competition and Bureau of Consumer Protection — and new enforcement powers for the Commission under §17 (a) and (b) would risk doing. While an eventual U.S. federal privacy bill will require one or multiple regulators for enforcement functions, any statutory powers should be balanced by increased Congressional oversight and monitoring mechanisms to hold such regulator(s) accountable.

Finally, a major feature of the proposed law is that any "Federal, State, Tribal, or local government entity" would be exempt from proposed rules under §2 (10) (C). However, at a time when government entities have emerged as a major source of data breaches and surveillance of Americans, privacy obligations should apply to both private and public entities. According to a survey of U.S. adults in May 2023 from the non-partisan Pew Research Center, 77 percent of Americans responded that they have "little to no understanding" about what the government does with their data (compared to 67 percent for companies), while 71 percent are "concerned" about how the government uses such data (compared to 81 percent for the private sector). As more cases of government surveillance and data breaches come to light, it is likely that concerns about how government entities collect and use data about Americans will continue to grow further.

While some exceptions might be needed in emergencies and on well-defined national security, such cases should be exceptions, not the norm, and formal criteria for such exceptions should be established in statute. Indeed, notwithstanding many negative aspects of the European Union's General Data Protection Regulation (GDPR), one positive aspect has been that its obligations apply both to government and private entities, albeit with some well-defined exceptions on national security and public safety grounds. Instead of mandating wholesale exemption for government entities, the revised APRA should ensure that data of U.S. residents and taxpayers from unlawful activities of government and non-government entities alike.

H.R. 7891 - the Kids Online Safety Act (KOSA) - and **H.R. 7890** - Children and Teens' Online Privacy Protection Act (COPPA 2.0)

Congressional efforts to protect online safety and privacy for young people are laudable. However, as was the case under previous versions of the legislation, the recently reintroduced KOSA and the amended COPPA 2.0 would significantly increase online surveillance and undermine privacy for youths and adults alike.

The central problem with these two bills is that, in seeking to address the current lack of data protection and online privacy, they will inevitably result in more tracking of users. By holding online platforms liable for all sorts of societal ills – from anxiety and depression to eating and substance use disorders, the two bills would force online platforms to snoop on users and restrict online speech. While online safety and privacy must be improved, even more surveillance is not the answer.

II. Contact Information

Thank you for your consideration. Should you have any questions about the content in this memo, please do not hesitate to reach out to Ryan Nabil, rnabil@ntu.org.