To: Members of the House Committee on Energy and Commerce's Innovation, Data, and Commerce Subcommittee
From: National Taxpayers Union
Date: May 22, 2024
Subject: NTU's Views on May 23 Subcommittee Mark-up of American Privacy Rights Act (APRA)

I. Introduction

On behalf of the National Taxpayers Union (NTU), the nation's oldest taxpayer advocacy organization, we write to express our views on the American Privacy Rights Act. NTU applauds the Committee for your continued efforts to advance legislation that will protect taxpayers' data privacy. However, given a number of concerns associated with this legislation, NTU urges caution and suggests several reforms as the legislative process proceeds on this bill.

II. Key Taxpayer Considerations

Against the backdrop of a growing patchwork of state privacy laws, the American Privacy Rights Act, introduced 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 states.

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.

III. Proposed Amendments

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 under §19 (a).

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.

Likewise, the proposed civil rights enforcement powers for the FTC could exacerbate these regulatory challenges. Under §13, the Commission can pursue enforcement actions even when it merely suspects that a particular algorithm has vaguely defined "discriminatory effects." While any potential human rights violations and discrimination are important issues that must be taken seriously and addressed through current legal frameworks, granting the FTC arbitrary powers might not be the best way to pursue such goals, especially at a time when the agency is routinely accused of regulatory overreach and acting beyond its legal mandate.

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, considering that 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 respondents reported that they have "little to no understanding" about what the government does with their data (compared to 67 percent for data use by companies), while 71 percent have expressed concern about how the government uses such data (compared to 81 percent for companies). 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 for well-defined national security reasons, 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, one positive aspect is that its obligations apply to both government and private entities, albeit with some well-defined exceptions for national security and public safety. Instead of mandating wholesale exemption for government entities, the revised APRA should ensure that the personal data of U.S. residents and taxpayers are protected from unlawful activities by both government and non-government entities. Therefore, Congress should consider i) removing the exemptions for government entities under §2 (10) (C), or ii) specifying the national security and public safety grounds under which government entities would qualify for exemption and the criteria these entities must meet to qualify for such targeted exemptions.

IV. 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.