CENTER FOR DEMOCRACY & TECHNOLOGY

Jessica Herron
Clerk, Innovation, Data, and Commerce
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515
Via email

Wednesday March 29, 2023

Re: QFR Responses for Hearing Entitled "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy", March 1, 2023.

Dear Ms. Herron:

Thank you for the invitation to appear before the Subcommittee on Innovation, Data & Commerce to testify during the March 1, 2023 hearing entitled "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy."

Pursuant to the Committee's Rules, I have been asked to answer an additional question for the record, my response to which is attached.

Sincerely,

Alexandra Reeve Givens

Written Responses - Question for the Record
Alexandra Reeve Givens
President & CEO, Center for Democracy & Technology

For the U.S. House of Representatives Energy & Commerce Committee,
Subcommittee on Innovation, Data, & Commerce
Hearing Entitled "Promoting U.S. Innovation and Individual
Liberty through a National Standard for Data Privacy"
March 1, 2023

The Honorable Diana Harshbarger

Question: As more and more connected technology devices are increasingly tracking human behavior and producing more and more data, do you think consumers should have ownership over this data?

Data ownership, while appealing in theory, is difficult to operationalize. One of the complicating factors is that data is a "non-rivalrous" good: copies of the same data can exist in multiple locations and be accessible by multiple people or entities, without necessarily jeopardizing each one's ability to make use of the data. For non-rivalrous goods, a property framework may not always be the best answer, particularly given how easy it is to copy data online. Further, allowing people to sell their data would benefit only the biggest online players, as large companies like Meta and Alphabet can surely afford to purchase the rights to use people's data from their significant user bases, while smaller start-ups would find that more difficult. And last, there is no guarantee that any particular piece of data would be worth more than a negligible amount, so it is unlikely that people would be compensated in a meaningful way. Large datasets are valuable because they allow for statistical analysis yielding insights about people or groups of people, but each individual data point, on its own, may not be worth much.

A more effective approach is to give people rights over data that pertains to them: rights to access, delete, correct, and port that data. These rights give people the ability to know what companies collect about them, and have the ability to correct it if it's wrong, delete it if they no longer want the company to have it, or port the data to another service provider. These rights have more meaning and value than the ability to own and sell data for fractions of a penny. They must, however, be enforceable, which is why a private right of action is such an important component of any federal privacy law (since the FTC and State Attorneys General are unlikely to prioritize these issues over other enforcement priorities).

However, the most important protections in any federal privacy law are data minimization and purpose limitation: prohibiting businesses and other entities from collecting more data than what is necessary to provide the service a person has requested. For example, an online retailer needs to collect customers' shipping information, payment details, contact information, and details about the product being sold. It does not need detailed demographic information about

the customer or data about other websites they have browsed, and should not collect and retain that data (let alone share or sell it to unknown third parties, as can happen now).

To expand on this point, our hypothetical online retailer should not be allowed to sell its customers' purchase records to a data broker, which might then combine all of a person's purchase records, aggregated from various retailers, and any other information the broker can amass including location and demographic data, to create a detailed dossier of someone's online and offline life. Such a record is likely to reveal sensitive information about that person's likes and dislikes, health conditions, political opinions, religious affiliation, and more. When such records can be sold on the open market to any willing buyer (including large tech companies and foreign governments), they are ripe for exploitation and abuse. A data ownership framework is unlikely to meaningfully address these harms, but a robust federal law prohibiting such data practices can give consumers the protections they need.