March 31, 2023

Jessica Herron
Legislative Clerk
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Re: Jessica L. Rich's Responses to Additional Questions for the Record

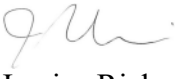
Dear Ms. Herron:

I want to thank the Subcommittee for inviting me to appear before it on March 1, 2023 to testify on the topic of "Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy." It was an honor to testify, and your assistance both before and after the hearing was especially helpful.

Pursuant to the Rules of the Committee on Energy and Commerce, I am attaching my answers to additional questions for the record, in the required format.

Thanks again for your help, and please let me know if you have any questions.

Sincerely,



Jessica Rich
Of Counsel and Senior Policy Advisor for Consumer Protection
Kelley Drye & Warren LLP

Attachment 1—Additional Questions for the Record

The Honorable Diana Harshbarger

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?

In theory, yes, consumers should own and control their data because of the adverse consequences that can result when that data is misused. However, one problem with an ownership model is that it would likely impose enormous burdens on consumers to manage their data and their privacy, including in each interaction they have with hundreds of companies. This could become completely unworkable, as we have learned from our experience with the notice-and-choice model for privacy. Indeed, the notice-and-choice model, while designed to give consumers more control over their data, ends up overwhelming them with hundreds of long and confusing privacy notices.

That's why there is so much support for the bipartisan ADPPA, which seeks to reduce these burdens on consumers and instead impose more duties on companies to follow responsible data practices, such as the duty to conduct privacy impact assessments; the duty not to discriminate; and restrictions on the use of sensitive data.

The Honorable Russ Fulcher

Building on our discussion in the hearing and specific to the American Data Privacy and Protection Act. In that act, certain entities are required to submit impact assessments to the FTC related to algorithms.

1. **Currently, does the FTC have the ability to request information that would be included in the impact assessments using their own authority and also permit entities to submit such information in a manner that doesn't expose trade secrets?**

Yes, the FTC has the authority to request a wide range of information (under the FTC Act and the FTC's Rules of Practice) in order to determine whether there have been law violations. The FTC also has the authority to conduct studies, such as the one it is current conducting on Pharmacy Benefit Managers (PBMs).

Many of these investigations and studies involve sensitive information and trade secrets, including (in addition to the PBM study) investigations and studies regarding merger and other antitrust issues; data security and privacy; and health products and health claims. The law and FTC rules allow companies to mark information as "confidential" (such as when it involves trade secrets) so that it receive special treatment and confidential handling. See here for a summary.

How would the FTC handle receiving all of these impact assessments if companies would be required to submit every assessment versus the FTC asking for it on their own accord?

Currently, the FTC obtains and reviews many third-party assessments, pursuant to its privacy and data security orders. While some of these assessments are automatically submitted to the agency, others are obtained by the FTC on request. In my experience, the FTC *does* frequently ask for and review even those assessments that aren't automatically submitted. Nevertheless, the assessment requirements under the ADPPA, which apply to any entity meeting a certain size threshold and not just those under an FTC order, would significantly add to the FTC's duties here. For the FTC to perform this work effectively, it would require more resources.

I wanted to ask you about the importance of ensuring the ability for businesses to continue to innovate. I want to give you more time to address the question below.

In the years since GDPR went into effect, we have seen the fall out in the EU. Large businesses continue to grow larger while small businesses and startups are becoming a rarity.

2. **How can we ensure this does not happen within the United States?**

Innovation is a hallmark of the US economy, and any privacy law enacted in this country should ensure that innovation continues to flourish. By necessity, that includes ensuring that small businesses can continue to compete and serve their communities.

One part of the solution is enacting a federal privacy law that sets a consistent standard, rather than forcing companies to navigate and develop costly compliance schemes for multiple different state laws. While compromise on preemption seems necessary in order to pass a federal law, the law still should try to achieve as much consistency as possible.

Another part of the solution is to limit the compliance costs on small businesses. Indeed, many existing privacy laws actually favor large companies, due to the high cost of compliance or because they focus unduly on limiting data-sharing with third parties (something large companies can avoid by keeping their functions in-house). The ADPPA attempts to avoid these effects by placing less emphasis on third-party sharing (in favor of more even-handed restrictions on data misuse) and by scaling down some of the duties for small businesses. For example, the bill reduces the burdens on small businesses when it comes to the data portability and correction, data security, executive responsibility, and audit and assessment requirements.