WRITTEN RESPONSES – QUESTIONS FOR THE RECORD

Graham Mudd
President & Chief Product Officer
Anonym, Inc

FOR THE

Subcommittee on Innovation, Data, and Commerce
Committee on Energy & Commerce
United States House of Representatives

HEARING ON

Promoting U.S. Innovation And Individual Liberty Through A National Standard For Data Privacy

March 1, 2023

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?

Yes, I do believe that consumers should have more ownership and control over the data they generate – and that this issue will only become more important as Americans' use and reliance on connected devices deepens. Unlike physical property, data is infinitely replicable, which means it can be reproduced and shared with additional parties at very little cost. This means consumers can very quickly and easily lose any measure of control over their data. Without federal legislation in place, consumers have little assurance that data they generate and share with one party won't be shared with others and put to use in ways that may harm them. For example, in the digital advertising industry, data is a powerful asset, so there is a strong incentive for companies to share data with the platforms through which they advertise. As a result, advertising technology companies and data brokers build and maintain incredibly deep profiles of people' online and real-world behavior. These profiles can be used in ways that are counter to an individual's interests.

The Honorable Russ Fulcher

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.

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

Many would argue that GDPR was overly burdensome to small businesses, particularly relative to the potential privacy harms that these businesses are capable of inflicting. There are a number of potential lessons that can be drawn from GDPR, many of which are already addressed in the latest draft of ADPPA.

For example, the most significant compliance requirements should be focused on the entities whose data practices have the potential to affect the greatest harm. Data volume is one dimension to consider. For example, entities that collect data from many other companies to develop consolidated profiles on millions of individuals are worthy of more regulatory focus than small businesses who maintain information on a modest customer base.

The sensitivity of the data handled by an entity is another dimension to consider. Companies that handle health or financial information should reasonably be subject to stricter compliance requirements than businesses that handle de-identified or less sensitive data.

ADPPA recognizes both of these dimensions and requires more of companies that handle either large volumes of data or sensitive data than those which do not. For example, small businesses, as defined by

ADPPA, are exempt from requirements to provide consumers with the right to request or correct their data, and from the requirement to establish a data privacy or security officer.

It's also important to proactively support small businesses in their compliance efforts. The ADPPA requires the FTC to develop a compliance program – this program should devote considerable resources to supporting small businesses.

In addition, Congress and regulatory agencies should encourage the development of technologies that support the adoption of privacy preserving practices (sometimes called "privacy-enhancing technologies," a.k.a. "PETs"). This can make privacy compliance easier for small businesses that don't have deep in-house privacy expertise. It also can level the playing field for small businesses that want to leverage data for analysis without compromising customers' privacy.

Thank you for your expertise. I know that the digital ecosystem runs on information, but sometimes it seems companies and data brokers are collecting more information than they need.

2. *Can you explain what information companies are collecting, what information they are using, and if they aren't using everything, why collect more information than they are actually using?*

It's difficult to answer your question about what is collected other than to say "everything." If a given behavior or attribute is digitally observable, then it is more than likely collected.

Without regulations in place, it is often the case that there are strong incentives to collect more information than might be immediately or obviously useful. This is because collecting and storing information is typically extremely inexpensive and unforeseen new applications for already-collected data are likely to arise in the future. For example, machine learning can be used to discover correlations that help a business make a prediction about consumer behavior that are far from obvious to humans.

Data minimization requirements, such as those included in ADPPA, provide a necessary incentive to reduce the collection, storage and transfer of data that isn't strictly necessary for an allowed purpose. These requirements can, and should, encourage companies to de-identify and anonymize data, which meaningfully reduces privacy risks while still supporting most applications and uses.