September 19, 2018

Honorable John Thune
Chairman, Committee on Commerce,
Science, and Transportation
United States Senate
Washington, D.C. 20510

Honorable Bill Nelson
Ranking Member, Committee on Commerce,
Science, and Transportation
United States Senate
Washington D.C. 20510

Dear Senators

Thank you for scheduling next week's hearing on "Examining Safeguards for Consumer Data Privacy."[1] We write today to emphasize the importance of Congressional action on data protection in the United States. We are disappointed that the September 26 hearing currently includes only voices from private industry. We strongly urge the Committee to include academics and representatives from civil society with expertise in data protection.

Current Inadequacies in United States Law

In the current digital age, companies have access to substantially more data about individuals than at any time throughout history, a reality becoming aggressively worse with the continued introduction of "internet of things" devices into our daily lives. While many governments around the world have responded by implementing data protection laws, the United States lags behind. The U.S. has instead established a "sectoral" approach to privacy adopted over time. This means that, at a federal level, we have implemented a patchwork of laws that provide some protections for certain types of data, like data pertaining to students or health information. There is no blanket protection from unchecked data collection, misuse, manipulation, or abuse. In its absence, we have relied on authority given to the Federal Trade Commission ("FTC") to pursue companies that engage in unfair or deceptive trade practices.

This status quo is inadequate at meaningfully protecting users from threats to their data. Take, for example, the circumstances between Cambridge Analytica and Facebook that has received attention as of late.[2] Earlier this year, it was revealed that Cambridge Analytica retained personal information of approximately 87 million (or more) Facebook users that it had received from researcher Aleksandr Kogan through an app he had designed using Facebook's API ("application programming interface"). The app allowed Kogan to access personal information not only about app users but also their Facebook friends, who had not, and in fact could not have, consented to the use of their data. Cambridge Analytica analyzed and used the data to create and purchase highly targeted ads that were used for the 2016 U.S. presidential elections, as well as potentially for other high-profile elections and debates. Company executives have

[1]https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=240B5C17-CBD5-4039-A9E4-CF2FADFF4712.
[2]https://www.accessnow.org/its-not-a-bug-its-a-feature-how-cambridge-analytica-demonstrates-the-desperate-need-for-data-protection/.

claimed that Cambridge Analytica has been involved in elections around the world, including the U.K., Argentina, India, Mexico, Nigeria, Kenya, and the Czech Republic.

The data at issue in this example did not fall into one of the limited areas where the United States has legislated on privacy. Additionally, at the time that this incident occurred, Facebook was already subject to a consent decree with the FTC which was neither able to prevent it nor did it ensure timely remedy.[3] Notably, one of the standard clauses in FTC consent decrees, including the one with Facebook, is the requirement for an independent audit (or assessment). While these audits may have been able to provide a means for responding to this and similar incidents, experts have flagged their deficiencies:

> *"These audits, as a practical matter, are often the only "tooth" in FTC orders to protect consumer privacy. They are critically important to accomplishing the agency's privacy mission. As such, a failure to attend to their robust enforcement can have unintended consequences, and arguably, provide consumers with a false sense of security."*[4]

Data Protection in the United States

Strong federal data protection legislation is needed to remedy these shortcomings in U.S law. Such a standard not only will respond to increasingly important needs, but it will provide protections for people in the United States on par with those that people enjoy in an ever-growing number of other countries and regions, including the whole of the European Union. A data protection law will also demonstrate that data stored by companies in the United States will adequately protect user information, assisting with ensuring free flows of data across geographic borders. Finally, a law can provide important guidance and clarity for private industry in this important area.

In order to provide meaningful protections for individuals, data protection legislation must combine a series of affirmative rights with affirmative obligations for entities that process data. Appropriate legislation should also include a series of government investments to incentivize research and development into privacy-protective practices and behaviors and helping position the United States as a leader of data protection.[5]

We have identified several provisions that we believe should be a part of any data protection proposal.[6] Some of these provisions include:

---

[3]https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[4] https://cyberlaw.stanford.edu/blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders.

[5] Unfortunately, none of the current legislative proposals pending in Congress provides for the necessary levels of user protection. To view our complete analysis of current bills, *see* https://www.accessnow.org/cms/assets/uploads/2018/04/USG-Data-Protection-Bills.pdf.

[6] The full list of our recommendations is available at https://www.accessnow.org/data-protection-in-the-united-states-where-do-we-go-from-here/.

- **Individual rights to information, access, rectification, portability, and erasure** - ensuring that people who have their data process have the ability to know what data has been collected, rectify incorrect data, and easily change or leave services
- **Government investment** - incentives for companies who pursue privacy-protective business models and practices, including through grant programs and preferences in bidding for government contracts
- **Building and strengthening federal agencies** - pursuing the development of an independent data protection commission with authority over implementation of the law as well as ability to conduct investigations and issue sanctions; direction of this new agency or an existing body to conduct research into the short- and long-term consequences of data breaches, including breaches of non-financial information
- **Data breach notification** - a blanket federal standard to require general public notification of all data breaches, with individualized notification for breaches that could result in potential harm, including emotional harm
- **Corporate obligations for obtaining consent and limiting data collection** - implementing requirements that require specific, enumerated reasons to allow collection of data and ensuring that it is only collected pursuant to meaningful, informed, uncoerced consent

The need for academic and civil society representation

It is important to note that the scheduled hearing is set to include *only* voices from private industry, including major players in the data ecosystem like AT&T, Google, and Amazon. Data protection may provide benefits to private industry in the form of certainty and standardization of international obligations. However, while data protection is inherently a concept that stands to protect the data of individuals, corporate interests do not align with the interests of people on this area. In fact, recently three major trade groups have published “principles” for data protection, with each of them falling short of any set of standards supported by groups who represent individual interests, including the provisions that we describe above.

In order to ensure a comprehensive hearing that provides committee members with important viewpoints and areas of expertise, we highly recommend the addition of advocates, academics, and independent data protection experts. While we believe it is most effective to include these perspectives on the panel alongside the corporate interests to allow for conflicting positions to be aired and ensure equal attention from committee members, a second panel could also be added, at a minimum, to secure an inclusive reflection on the issues.

Thank you again for your time and attention to this important matter. We appreciate your serious consideration of data protection and are available to provide any additional information or analysis that may be useful to committee members.

About Access Now:

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[7] By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. Access Now maintains presences in eleven cities around the world, including in the policy centers of Washington, DC and Brussels.

Sincerely,

Amie Stepanovich
U.S. Policy Manager

[7] accessnow.org.