April 9, 2020

Privacy Recommendations for Pandemic Response

Submitted to the Senate Commerce Committee on behalf of the Privacy and Digital Rights for All Coalition in response to the paper hearing entitled "Enlisting Big Data in the Fight Against Coronavirus"

Data policy will be central to the response to the coronavirus pandemic. New data collected as a result of the pandemic and existing data repurposed for pandemic response must be regulated to protect individual rights and prevent uses inconsistent with public health.

Congress should ensure the following safeguards:

- Data collected by the government and through public/private partnerships must be the minimal amount necessary to accomplish the public health purpose for which it is collected. Any business that participates in a public/private partnership must confirm that it will adhere to existing law and the below additional privacy and security guidelines before entering the partnership.

- Individuals must have certain rights over information collected from or about them during or as a result of the pandemic. These rights should cover data collected in a business's normal course of operations but used, shared, or processed in new ways during the public health crisis (for example, geolocation data), as well as data collected for new purposes related to the pandemic. Individuals should be informed in clear and plain language the purpose of the data collection, how the data will be used or processed, how the data will be secured and for how long the data will be maintained, and should be able to easily access data that has been collected about them promptly and free of charge. It should be unlawful for a business to raise prices or otherwise retaliate against anyone who exercises these rights.

- Data collected as a result of the pandemic should never be used for purposes unconnected to public health. Particularly commercial purposes (such as marketing and advertising), purposes not strictly necessary for public health (for example law or immigration enforcement), or to inappropriately target vulnerable populations. Pandemic related data collection and processing must never facilitate discrimination or other abuses of human rights.

- Data that has been collected, processed, or combined in ways that would not have been permitted except for the crisis must be automatically deleted once the crisis is over. Such data must never be shared or used for other purposes. These limitations should cover data collected, processed, or combined for financial purposes, such as the provision of relief packages or special financial products to consumers and small businesses during the crisis. Moreover, as consumers' credit reports and financial privacy are currently threatened for reasons that have nothing to do with their general creditworthiness, all negative credit reporting should cease.

- Penalties for violating these standards must be severe. Heightened penalties should apply when the offense involves the targeting or processing of data of vulnerable populations while the health crisis is ongoing, and during any resulting economic slowdown. The consequences for data breaches and violations should be tough enough to make sure that data is held securely, and that the financial benefits of violating the law never exceed the consequences. The FTC, State Attorneys General, and private litigants should all have a role in enforcing the privacy protections put in place, and there should be strong independent oversight of processing entities during the crisis. Insights or intellectual property gained from these efforts should remain in the public trust.

Thank you for your attention to this important topic.

Our privacy laws are decades out of date. The Privacy and Digital Rights for All Coalition is dedicated to advocating for a new approach to privacy protections. For more information about our coalition, see our principles and list of members at https://www.citizen.org/about/coalitions/digitalrights4all/.