May 5, 2020

The Honorable Michael R. Pence
Vice President of the United States
The White House
Offices of the Vice President
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Vice President Pence:

As leading civil society organizations, we represent individuals and communities in every part of the United States whose lives are being upended and threatened by COVID-19. We support the efforts at all levels of government to combat the pandemic and recognize the vital role of the Federal government to provide leadership and set guidelines for responding to this crisis. Crucial elements of that response include free and widely available testing, equitable access to healthcare, contact tracing, data analytics and technologies, and communicating clearly and transparently to the public about how these measures work. Building appropriate privacy safeguards into the systems that are created to carry out these efforts and being transparent about the collection and use of personal and aggregate information are essential to garnering the public's trust and cooperation and to ensuring that the benefits of this response are shared equitably among all.

While technology can be helpful in these efforts, it is not a "silver bullet"[1] and its use can undermine fundamental American values such as privacy, equity, and fairness. Before rushing toward a technological fix, there must be consensus among all relevant stakeholders on the most efficacious solution. The proper use of technology, personal and aggregate data, and data analytics has the potential to provide important public health benefits, but it must incorporate proper privacy and security safeguards, as well as protections against discrimination and violations of civil and other rights.

The absence of federal baseline privacy legislation covering the private sector makes the call for proper safeguards even more important and urgent. This has led to an explosion of privacy violations and other harmful or manipulative data practices and underscores why we must ensure that an initiative to fight the COVID-19 pandemic is not executed without safeguards to ensure privacy, equity and fairness. Many experts, advocates, and academics in the United States and around the world share these concerns, and they were recently expressed on a bi-partisan basis in Congress.[2]

Concerns have also been raised about public-private partnerships (PPPs) that use technology to provide information and assistance to the public about COVID-19 without the necessary privacy safeguards. Since PPPs are not subject to the Privacy Act of 1974 which covers federal agencies and may otherwise not fall under other privacy legislation, federal, state, and local agencies should establish and enforce

[1] *See* Janosch Delcker, *Coronavirus: Actually, we don't have an app for that*, Politico (April 23, 2020, updated April 24, 2020), https://www.politico.eu/article/coronavirus-smartphone-apps-alone-wont-help-curb-the-pandemic-artificial-intelligence-experts-warn/.

[2] *See* https://www.commerce.senate.gov/2020/4/enlisting-big-data-in-the-fight-against-coronavirus, U.S. Senate Committee on Commerce, Science & Transportation (April 9, 2020).

comprehensive privacy and security standards for the PPPs they enter into.[3] For example, Project Baseline,[4] the initiative by Alphabet subsidiary Verily in collaboration with the California governor's office to create a website that provides information to the public about local coronavirus testing, came under fire[5] because individuals must have a Google account to use the website and there is nothing to prevent Google or Verily, which are not "health care providers" covered by the Health Insurance Portability and Accountability Act, from using and sharing the personal information they collect about individuals for other purposes.

We urge the federal government to adopt these principles in its own response to COVID-19 and use them as the basis for standards that other government agencies and the private sector can follow:

- **Set science-based, public health objectives to address the pandemic**. Then design the programs and consider what tools, including technology, might be most efficacious and helpful to meet those objectives.
- **Assess how technology and other tools meet key criteria.** This should be done before deployment when possible and consistent with public health demands, and on an ongoing basis. Questions should include: Can they be shown to be effective for their intended purposes? Can they be used without infringing on privacy? Can they be used without unfairly disadvantaging individuals or communities? Are there other alternatives that would help meet the objectives well without potentially negative consequences? Use of technologies and tools that are ineffective or raise privacy or other societal concerns should be discontinued promptly.
- **Protect against bias and address inequities in technology access.** In many cases, communities already disproportionately impacted by COVID-19 may lack access to technology, or not be fairly represented in data sets. Any use of digital tools must ensure that nobody is left behind.
- **Set clear guidelines for how technology and other tools will be used**. These should be aimed at ensuring that they will serve the public health objective while safeguarding privacy and other societal values. Public and private partners should be required to adhere to those guidelines, and the guidelines should be readily available to the public.
- **Ensure that programs such as technology-assisted contact tracing are voluntary.** Individual participation should be based on informed, affirmative consent, not coercion.
- **Only collect individuals' personal information needed for the public health objective.** No other personal information should be collected in testing, contact tracing, and public information portals.
- **Do not use or share individuals' personal information for any other purposes.** It is important to avoid "mission creep" and to prevent use for purposes unrelated to the pandemic such as for advertising, law enforcement, or for reputation management in non-public health settings.
- **Secure individuals' personal information from unauthorized access and use.** Information collected from testing, contact tracing and information portals may be very revealing, even if it is not "health" information, and security breaches would severely damage public trust.

---

[3] *See* Rebecca Adino and David Carpenter, *Protecting Privacy in Public Private Partnerships: What Government Agencies Should Know*, IAPP, (March 1, 2008) https://iapp.org/news/a/2008-03-government-agencies-protecting-public-private-partnerships/

[4] *See* https://www.projectbaseline.com/study/covid-19/.

[5] *See* Andrea Peterson and Emily Birnbaum, *Verily's COVID-19 website becomes a privacy battleground*, Protocol, (April 1, 2020) https://www.protocol.com/verily-coronavirus-website-test-menendez.

- **Retain individuals' personal information only for as long as it is needed**. When it is no longer required for the public health objective, the information should be safely disposed of.
- **Be transparent about data collection and use.** Before their personal information is collected, individuals should be informed about what data is needed, the specific purposes for which the data will be used, and what rights they have over what's been collected about them.
- **Provide accountability.** There must be systems in place to ensure that these principles are followed and to hold responsible parties accountable. In addition, individuals should have clear means to ask questions, make complaints, and seek recourse in connection with the handling of their personal information.

Protecting individuals' privacy, ensuring equity in the treatment of individuals and communities, and communicating clearly about public health objectives are complex challenges. As part of the Coronavirus Task Force, we urge you to immediately create an interdisciplinary advisory committee comprised of experts from public health, data security, privacy, social science, and civil society to help in developing the standards we are calling for. We also ask that the Coronavirus Task Force be fully transparent about its plans and request a meeting to discuss our concerns further. Opening the process and listening to a wide group of stakeholders will help foster trust and confidence in the programs that are being implemented to combat COVID-19.

Sincerely,

Campaign for a Commercial Free Childhood
Center for Democracy & Technology
Center for Digital Democracy
Constitutional Alliance
Consumer Action
Consumer Federation of America
Electronic Privacy Information Center (EPIC)
Media Alliance
MediaJustice
Oakland Privacy
Parent Coalition for Student Privacy
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
Rights x Tech