MICHAEL F. BENNET
COLORADO

COMMITTEES:
AGRICULTURE, NUTRITION, AND FORESTRY
FINANCE
INTELLIGENCE

United States Senate
WASHINGTON, DC 20510–0609

WASHINGTON, DC:
261 Russell Senate Office Building
Washington, DC 20510
(202) 224-5852

COLORADO:
Cesar E. Chavez Building
1244 Speer Boulevard
Denver, CO 80204
(303) 455-7600

http://www.bennet.senate.gov

April 30, 2020

The Honorable Mark Meadows
Chief of Staff
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dr. Robert R. Redfield
Director
Centers for Disease Control and Prevention
1600 Clifton Road
Atlanta, GA 30329

The Honorable Alex Azar
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Mr. Meadows, Secretary Azar, and Director Redfield:

The outbreak of Coronavirus Disease 2019 (COVID-19) has forced governments to explore bold and innovative strategies to protect both lives and livelihoods. The result is a proliferation of initiatives across the globe to fight the pandemic by applying digital technologies to existing tools for public health surveillance, such as contact tracing. As governments worldwide develop and deploy these technologies, the United States has an opportunity to lead. We must set an example to the world, not only by adhering to established, evidence-based standards for public health surveillance, but by also balancing the potential value of digital tools with their limitations and risks.

Cases abroad underscore the risk to privacy and civil liberties of bluntly applying modern technologies to public health surveillance. To fight the pandemic, the South Korean government pulled Closed Circuit Television (CCTV) footage for contact tracing and augmented public health data with data from personal credit cards, phone records, and location tracking applications. The Israeli government provided cell phone location data to its internal security services to identify those who needed to quarantine. Singapore and Taiwan have implemented similar policies.

We know from our recent history that, in the context of national security, a rush to respond in times of national emergency can establish an enduring precedent. After September 11, 2001, Congress granted the federal government sweeping new powers to monitor and collect personal data. Nearly two decades

later, several of these powers have never been meaningfully reexamined, while others have been repurposed in ways Congress never originally envisioned.

We must weigh these risks against the urgent need for creative solutions to address this and future pandemics. Therefore, the question we face is how to unlock the potential benefits of technology-driven public health surveillance without undermining Americans' personal freedoms and, ultimately, trust in our public health system.

Indeed, effective public health surveillance ultimately requires the cooperation and trust of individuals and communities whose data must be collected. If people fear the government will misuse their data, they may avoid testing and withhold critical information, jeopardizing our response to the pandemic and endangering the health of our communities.

As the administration considers how to apply emerging and existing technologies to fight the pandemic, I urge you to adopt the following principles to shape any public, private, or cross-sectoral effort going forward:

- **Choice:** Americans must be given the choice to opt-in to any data collection related to COVID-19 and have a clear right to refuse. Individuals must also have the right to remove their data if they choose.

- **Minimization**: Data collection at any level of government must include only the minimally required amount of personal information needed to fight COVID-19, as determined by public health experts.

- **Precedent:** Management of public health data should follow established protocols, whereby local and state entities serve as the primary data collectors and stewards and share only aggregated, anonymized data with the Centers for Disease Control and Prevention (CDC) for public health surveillance.

- **Fencing**: At the federal level, the CDC must remain the sole entity responsible for management and use of data related to COVID-19. Any private third party, state government, or other federal department, including law enforcement or national security agencies, shall not have access to federal data or management of such data. To protect privacy at every level, no other entity should combine, directly or indirectly, anonymized and aggregated data sets related to COVID-19 with other large data sets.

- **Sunset**: All personally identifiable information collected to fight COVID-19 must be deleted or de-identified upon termination of the disease cycle, as determined by public health experts.

- **Security:** All data collected must be secured with robust cyber-security and other measures, and data must be verifiable.

- **Non-discrimination**: Participation in the data collection must not determine, positively or negatively, an individual's access to testing, health care, or any other social services. No data must be used to discriminate on the basis of race, religion, nationality, immigration status, sexual orientation, or disability unless in the interest of that group.

- **Oversight**: Government public health agencies must provide strong oversight of any third-party applications designed to combat COVID-19 that involve the use of personal data with clear standards and enforcement mechanisms for privacy violations.

- **Public Use**: Any data collected must be used exclusively for the public benefit and must not be shared with third parties for monetization or private gain of any kind, including businesses, nonprofits, and consortia thereof.

- **Testing**: The effectiveness of any technologically-driven surveillance and mitigation strategies depends on the availability of universal testing, warranting greater federal government investment and attention.

- **Humility**: Any system must account for the limitations of technology and recognize the prevalence and risks of significant false positives and false negatives, for example, from widespread use of Bluetooth traces.

We are in a profoundly unsettled moment for America and the world. How nations apply modern technologies to this pandemic will set a precedent – for better or worse – that could last a generation. China has already deployed models that treat privacy and civil rights as afterthoughts. Given the stakes in human lives and freedoms, the United States and our allies must set the example for how to unleash the potential of technology to protect health and prosperity while also protecting democratic values. In doing so, we can lay the foundation to not only overcome this immediate crisis, but to leave the United States and the world more prepared and resilient to confront future pandemics.

Thank you for your urgent consideration of this matter.

Sincerely,

Michael F. Bennet