FUTURE OF PRIVACY FORUM
1400 Eye Street NW, Suite 450, Washington, DC 20005 | 202-768-8950 | fpf.org

September 9, 2020

National Committee on Vital and Health Statistics
3311 Toledo Road, Room 2402
Hyattsville, MD 20782

VIA EMAIL TO: NCVHSmail@cdc.gov

RE: 85 Federal Register 51455: "National Committee on Vital and Health Statistics (NCVHS), Hearing of the Subcommittee on Privacy, Confidentiality, and Security"

Dear Members of the National Committee on Vital and Health Statistics:

Thank you for the opportunity to provide comments in advance of the September 14, 2020 Hearing of the Subcommittee on Privacy, Confidentiality, and Security. Future of Privacy Forum (FPF) is a non-profit organization based in Washington, DC, with the mission of promoting privacy leadership and scholarship, and advancing principled data practices in support of emerging technologies.[1] FPF works on a range of consumer privacy issues, including connected wearable devices, health and wellness data, mobile apps and platforms, and the role of technology in addressing the COVID-19 pandemic. Through our *Privacy and Pandemics* series, we have been exploring the challenges posed by the COVID-19 crisis to existing ethical, privacy, and data protection frameworks.

We write to provide a number of existing resources that address the following issues raised by the Committee in the Request for Public Comments, including: (1) the application of the Fair Information Practice Principles (FIPPs) and proper scope of data collection, analysis, and sharing in an emergency; (2) differences in standards at the local, state, and federal levels; and (3) technical resources on understanding location data and the current design of mobile apps.

(1) Resources on the Fair Information Practice Principles (FIPPs) and Emergencies

Throughout our recent work, FPF has encouraged organizations and other stakeholders collecting digital contact tracing data to apply the Fair information Practice Principles (FIPPs)[2] to the collection and use of data for COVID-19. This includes limiting the scope of data collection to what is necessary and proportional to public health needs; adhering to purpose limitation principles; and promoting lawfulness and transparency through the use of privacy impact assessments (PIAs).

- Privacy and Pandemics: A Thoughtful Discussion (March 27, 2020). In this discussion, we provide the consensus advice from a *Privacy and Pandemics* Virtual Workshop in which FPF convened a dozen ethicists, academics, government officials, and corporate leaders,

[1] The views herein do not necessarily reflect those of our supporters or our Advisory Board.
[2] Records, Computers, and Rights of Citizens report of the U.S. Department of Health, Education and Welfare (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

as well as over 100 corporate attendees, to discuss responsible data sharing in times of crisis.

- FPF's testimony before the U.S. Senate Committee on Commerce, Science, & Transportation, Enlisting Big Data in the Fight Against Coronavirus (April 9, 2020). In this testimony, FPF explored how collection and uses of data, including personal data, to respond to a public health crisis like a pandemic can be compatible with privacy and data protection principles. We recommended that organizations collecting digital contact tracing data follow the lead of public health experts; ensure transparency and lawfulness; apply privacy enhancing technologies (PETs); employ privacy risk assessments (PIAs); and follow core purpose limitation principles.

- COVID-19 Public Work Session hosted by the Washington State Senate Committee on Environment, Energy & Technology (July 28, 2020). In FPF's recent presentation to Washington lawmakers, we recommended that policymakers and technology providers follow the lead of public health experts, and outlined key considerations and recommendations for how to design and implement digital contact tracing tools, including: purpose limitation; retention limits; privacy impact assessments; prioritization of accessibility; careful integration of external software development kits (SDKs); interoperability; and security.

- FPF and BrightHive's Digital Contact Tracing: A Playbook for Responsible Data Use (August 14, 2020). In this Playbook, we encourage organizations collecting digital contact tracing data to commit to limiting the scope of data collection according to the needs of public health experts. Decisions about which data, analytic, and technological models to pursue should be based on medical and public health partners' needs, their estimates of efficacy, and grounded in the best available evidence. We encourage stakeholders to limit the sharing of data to established partners who have demonstrated experience with responsible data sharing; and to be guided by the principles of necessity and proportionality.

(2) Resources on Differing Standards at State, Federal, Local Levels

In response to the ongoing public health emergency, organizations must comply with a wide range of existing regulations and standards, including Europe's General Data Protection Regulation (GDPR). In the United States, several federal proposals have been proposed, including the COVID-19 Exposure Notification Act. State legislatures have also been involved in emerging regulatory efforts to promote public trust and public participation by addressing concerns over the impact of digital contact tracing on privacy and civil liberties. Commercial entities using the Apple-Google Exposure Notification API must also comply with the privacy rules in the Terms of Service for those platforms.

The following FPF resources explore these topics:

- EU DPAs Issue Green and Red Lights for Processing Health Data During the COVID-19 Epidemic (March 10, 2020) – exploring how various European Data Protection Authorities issued public interest guidance on the limits of collecting, sharing and using personal data relating to health in these exceptional circumstances under the General Data Protection Regulation (GDPR).
- Newly Released COVID-19 Privacy Bills Would Regulate Pandemic-Related Data (May 15, 2020) — analyzing the Public Health Emergency Privacy Act (introduced by leading House and Senate Democrats) and the COVID–19 Consumer Data Protection Act of 2020 (introduced by leading Republicans), including its scope of covered data and entities; legal requirements; and a few key differences from its Republican counterpart.
- Bipartisan Privacy Bill Would Govern Exposure Notification Services (June 2, 2020) — analyzing the Exposure Notification Privacy Act, introduced by Senators Cantwell (D-WA), Cassidy (R-LA), and Klobuchar (D-MN), which would create legal limits for automated exposure notification services.
- Apple & Google Update Terms for COVID-19 Apps (May 27, 2020) — analyzing the privacy and security requirements of the Apple Google Exposure Notification API, designed for decentralized Bluetooth-based digital exposure notification apps. In September, Apple and Google also launched "Exposure Notification Express", making exposure notification functionality available at the operating system level.

(3) Additional Technical Resources

The following additional technical resources may provide helpful insights on the role of location data and the current design of mobile apps:

- FPF Charts the Role of Mobile Apps in Pandemic Response (April 3, 2020) — providing early analysis of the various objectives and methods of early digital contact tracing apps and software development kits.
- Infographic: Understanding the World of Location Data (May 22, 2020) — demonstrating how mobile devices interpret signals from their surroundings, including GPS satellites, cell towers, Wi-Fi networks, and Bluetooth, to generate precise location measurements.
- Thermal Imaging as Pandemic Exit Strategy: Limitations, Use Cases and Privacy Implications (June 3, 2020) — surveying the leading technologies, products, and use cases for thermal imaging, reviewing the technical limitations of thermal scanning as described in scientific literature, discussing the concerns articulated by privacy and civil rights advocates, and providing an in-depth overview of regulatory guidance on thermal imaging from the US, Europe, and Singapore.
- FPF's comments to the Office of Science and Technology Policy's (OSTP) (attached) advised that all federally funded research projects adopt a strong, risk-conscious, approach to privacy protections. We recommend that OSTP adopt a nuanced approach to requirements for fidelity to consent that acknowledges the limitations to consent and reinvigorates the use of consent documents to outline which research purposes conform to participants expectations. We recommend projects include language that outlines the potential privacy risks for reuse of the data, including results from a well-designed open

data risk-benefit assessment, and will clarify boundaries to privacy respecting reuse of the data.

Sincerely,

John Verdi
Vice-President of Policy
Future of Privacy Forum

Stacey Gray
Senior Counsel
Future of Privacy Forum

Pollyanna Sanderson
Policy Counsel
Future of Privacy Forum