epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

April 15, 2020

The Honorable Frank Pallone, Chair
The Honorable Greg Walden, Ranking Member
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Pallone and Ranking Member Walden:

We write to you regarding the protection of medical privacy amidst efforts to combat the spread of the novel coronavirus. The COVID-19 pandemic is a global health emergency of unprecedented scale, countries are deploying a wide range of techniques to respond. Congress should ensure that the pandemic is not used to justify expanded systems of location tracking and monitoring that undermine fundamental American values. The United States has an opportunity to lead the world by ensuring that digital technologies uphold civil liberties and human rights.[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] We have advised the U.S. Congress, state governments, and many international organizations, including the Organization for Economic Cooperation and Development ("OECD"), on new privacy challenges. Our advisory board includes distinguished experts in law, technology, and public policy. In the last month, we have worked closely with many experts, NGOs, and privacy officials on the challenges posed by the novel coronavirus.

Plans have begun to emerge, both in the United States and abroad, to ease social distancing restrictions and business closures.[3] These plans are varied, but they share key common elements: widespread testing, contact tracing, and targeted self-quarantines to limit the spread of new infections. Ultimately, the aim is the widespread availability and administration of a vaccines.

Need to Safeguard Privacy

It is essential that government agencies and private companies implement standards that safeguard privacy. As Dr. Michael Ryan of the World Health Organization has stated, there is a "tremendous amount" of innovation and enthusiasm for new products. But he also cautioned that

[1] *EPIC, Coalition Urge Governments to Respect Human Rights as They Respond to Pandemic* (Apr. 2, 2020), https://epic.org/2020/04/epic-coalition-urge-government.html; Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights (Apr. 3, 2020), https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight#; *see also* EPIC, *Council of Europe Issues Guidance on Fundamental Rights During Pandemic* (Apr. 8, 2020), https://epic.org/2020/04/council-of-europe-issues-guida.html.
[2] *About EPIC*, https://epic.org/epic/about.html.
[3] Scott Gottlieb, et al., *National Coronavirus Response: A Road Map to Reopening* (2020), https://www.aei.org/wp-content/uploads/2020/03/National-Coronavirus-Response-a-Road-Map-to-Recovering-2.pdf.

"when collecting information on citizens or tracking their movements there are always serious data protection and human rights principles involved."[4] Dr. Ryan said, "we want to ensure that all products are done in the most sensitive way possible and that we never step beyond the principles of individual freedoms and rights." As Effy Vayena, Professor of Bioethics at the Swiss Federal Institute of Technology (ETHZ) and co-chair of the WHO's expert advisory group on Artificial Intelligence, Health Ethics, and Governance, has explained, "[a]s big data will be critical for managing the COVID-19 pandemic in today's digital world, the conditions for responsible data collection and processing at a global scale must be clear."[5] She stressed that the "use of digitally available data and algorithms for prediction and surveillance" should be done "in a responsible manner, in compliance with data-protection regulations and with due respect for privacy and confidentiality."

The announcement last week by Apple and Google of a plan to create a standard to facilitate privacy-protective proximity tracing with a cell phone app could be an important first step, but the technological, legal, and policy impacts of such a system must be closely scrutinized. EPIC supports the deployment of genuine Privacy Enhancing Technologies that "minimize or eliminate the collection of personally identifiable information." But these techniques must be "robust, scalable, and provable."

These efforts at digital contact tracing, using apps or other data sources to track the contacts of individuals,[6] will present significant logistical, technological, and legal challenges; the onus should be on the governments, companies, or entities deploying these systems to prove that they are necessary, effective, lawful, and protect privacy. UK computer scientist Ross Anderson has warned that there are significant concerns about the security of the Apple-Google plan.[7] Former vice president Joe Biden has correctly said "there needs to be widespread, easily available and prompt testing — and a contact tracing strategy that protects privacy."[8]

Safeguarding Location Data

Location data is inherently sensitive, and Congress should ensure that it is protected.[9] Not only does it reveal the location of a particular person, location data also reveals when people are

---

[4] Remarks of Dr. Michael Ryan, World Health Organization, *Daily Brief* (Mar. 25, 2020), https://epic.org/privacy/covid/who/march25remarks.mp4; *See also*, EPIC, *WHO Advisor – "We Should Never Step Beyond Individual Freedoms* (Mar. 26, 2020), https://epic.org/2020/03/who-advisor---we-should-never-.html; EPIC, *World Health Organization Again Speaks Up for Data Protection* (Mar. 27, 2020), https://epic.org/2020/03/world-health-organization-agai.html

[5] Marcello Ienca & Effy Vayena, *On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic*, Nature Medicine (Mar. 27, 2020), https://www.nature.com/articles/s41591-020-0832-5.

[6] See Luca Ferretti, et al., *Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing*, Science (Mar. 31, 2020), https://science.sciencemag.org/content/early/2020/04/09/science.abb6936; Emily Waltz, *Halting COVID-19: The Benefits and Risks of Digital Contact Tracing*, IEEE Spectrum (Mar. 25, 2020), https://spectrum.ieee.org/the-human-os/biomedical/ethics/halting-covid19-benefits-risks-digital-contact-tracing.

[7] Ross Anderson, *Contact Tracing in the Real World*, Light Blue Touchpaper (Apr. 12, 2020), https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/. A copy of Ross Anderson's post is attached to this letter.

[8] *See* Opinion, *Joe Biden: My Plan to Safely Reopen America*, N.Y. Times (Apr. 12, 2020), https://www.nytimes.com/2020/04/12/opinion/joe-biden-coronavirus-reopen-america.html.

[9] Letter from EPIC to the House Committee on the Judiciary re: Privacy of Location Data (Feb. 14, 2020), https://epic.org/testimony/congress/EPIC-SJC-Location-Data-02142020.pdf.

together, who they may share a bed with, and other intimate facts. The use of digital contact tracing should satisfy four requirements:

(1) Participation should be lawful and voluntary;
(2) There should be minimal collection of personally identifiable information;
(3) The system should be robust, scalable, and provable; and
(4) The system should only be operated during the pandemic emergency.

This moment provides a unique opportunity to show that privacy and public health are complimentary goals and to establish that Privacy Enhancing Techniques can be deployed to serve the public interest and protect individuals.

Some of the current app-based contact tracing proposals could potentially meet these requirements if they are shown to be robust, provable, and scalable. Several of the proposals, including Singapore's TraceTogether app[10] and the Apple-Google proposal, use short-range Bluetooth signals to generate a digital contact log. TraceTogether was developed in conjunction with data protection authorities, includes many privacy safeguards, and makes data minimization a focus. One important element in these Bluetooth contact tracing proposals is the use of a random, rotating identification scheme. The purpose of this design is to avoid generating or collecting personally identifiable data. In contrast, proposals that would use existing phone location data (GPS) records, transactional records, or other persistent tracking methods would require the collection, disclosure, or use of vast amounts of sensitive personal information.

The Use of Location Data Implicates Constitutional Interests

Government agencies should not use the pandemic to justify the collection of large volumes of data about everyday Americans movements and locations. In 2018 the U.S. Supreme Court ruled in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), that the Government's warrantless acquisition of historical cell phone location records violated the Fourth Amendment. The Court has not yet had an opportunity to evaluate the standard for access to other types of location data, but Congress should closely scrutinize any expanded surveillance of Americans. And the Court's decision in *Carpenter* did not address the legal standard for companies' collection, use, and disclosure of sensitive location data to private entities. The FCC recently fined the three largest cell phone providers $200M for selling location records.[11]

The Court established in *Carpenter* and *Riley* that cell phone data is entitled to Fourth Amendment protections but also encouraged Congress to address this complex issue through legislation.[12] The Committee should act quickly on this matter.[13] Cell phones are an essential part of

[10] Gov't of Singapore, *Help Speed Up Contact Tracing with TraceTogether* (Mar. 21, 2020), https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether.
[11] Fed. Commc'ns Comm'n, *FCC Proposes Over $200M in Fines for Wireless Location Data Violations* (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations; *see* 47 U.S.C. § 222.
[12] *Carpenter*, 138 S. Ct. at 2496 (Alito, J., concurring) ("it would be very unfortunate if privacy protection in the 21st century was left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.").
[13] *See* Editorial Board, *The Government Uses 'Near Perfect Surveillance' Data on Americans*, N.Y. Times (Feb. 7, 2020), https://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html.

everyday life; we all use mobile apps for personal, financial, business, education, entertainment, and social activities. *Riley v. California*, 573 U.S. 373, 396 (2014). The Committee should ensure location data is protected in the context of comprehensive baseline legislation as set out in the Online Privacy Act H.R. 4978.

There are many circumstances where location data can be used in an aggregated, deidentified format for public health purposes. For example, differential privacy techniques are now being used to create anonymized metrics of changes in behaviors (visits to places like grocery stores and parks) in different countries and regions.[14] But it is essential that any system for creating "anonymized" data be robust, provable, and scalable. And governments should not seek to collect large volumes of identifiable data when they could instead rely on Privacy Enhancing Techniques.

Congress should investigate whether companies and government agencies involved in digital contact tracing and other pandemic surveillance programs are protecting the privacy of Americans. It is essential that use of tracking technologies in response to the pandemic are carried out strictly in line with civil liberties and human rights.

EPIC looks forward to working with the Committee on these and other issues concerning privacy and the pandemic response.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Alan Butler
Alan Butler
EPIC Senior Counsel

Cc: Chairman Janice D. Schakowsky, Subcommittee on Consumer Protection and Commerce
Ranking Member Cathy McMorris Rodgers, Subcommittee on Consumer Protection and Commerce

[14] Ahmet Aktay, et al., *Google COVID-19 Community Mobility Reports: Anonymization Process Description (version 1.0)*, arXiv:2004.04145v2 (Apr. 9, 2020), https://arxiv.org/pdf/2004.04145.pdf. Apple is also making mobility data available, which not connected to any persistent identifiers. Apple, *COVID-19 Mobility Trend Reports* (2020), https://www.apple.com/covid19/mobility.