ACT | The App Association

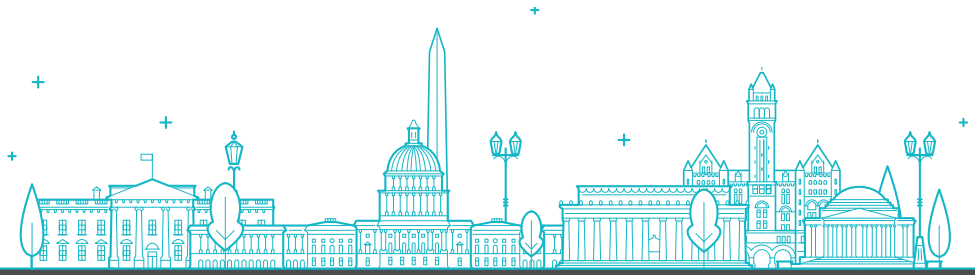
Enlisting Big Data in the Fight Against Coronavirus

Testimony of

Graham Dufault
Senior Director for Public Policy
ACT | The App Association

Before the

U.S. Senate Committee on Commerce,
Science, and Transportation



1401 K Street NW Suite 501
Washington, DC 20005
202.331.2130
www. ACTonline.org
@ACTonline
/ACTonline.org

I. Introduction

We thank the Senate Committee on Commerce, Science, and Transportation for holding this paper hearing on how governments, the private sector, and other stakeholders are leveraging big data to combat the novel coronavirus, which causes COVID-19. ACT | The App Association is the voice of small business tech entrepreneurs, and we appreciate the Committee welcoming us to share the experiences and perspectives of our member companies in combating and slowing the spread of this deadly disease. As of the time we submitted this written testimony, global deaths due to COVID-19 reached 76,507 with 1.37 million global confirmed cases.[1] And these numbers are sure to rise in the subsequent hours and days. The rapidly evolving threat to human life COVID-19 presents demands swift and effective responses by stakeholders across the globe, including the use of big data tactics.

The App Association is a trade group representing about 5,000 small to mid-sized software and connected device companies across the globe. In the United States, our member companies are part of a $1.7 trillion industry, supporting about 5.9 million jobs. They are on the front lines in the fight against COVID-19. They are adapting virtual care solutions for providers to help patients impacted by COVID-19, helping businesses work virtually, and—relevantly for this hearing—they are creating portals to enable big data analysis of patient risk factors and trends. Likewise, the App Association's Connected Health Initiative (CHI) is pushing for policy changes that would enable the use of digital health tools that both feed and leverage big data analytics.

As you examine the uses of big data to combat the novel coronavirus, we urge you to consider a few key concepts. First, experts are using big data to combat COVID-19 in a variety of ways, including to identify spread patterns and trends; to inform the development of treatments and a vaccine; and to forecast resource needs. Second, privacy concerns around the use of big data underscore both the need for governmental restraint in acting on data analytics and for governmental action to enact a national privacy framework. Third, digital health and telehealth tools inform big data insights while helping patients and consumers manage and avoid chronic conditions, underscoring the need to make these tools (and healthcare data) accessible to providers, consumers and patients.

II. Big Data, Targeted Impact

Identifying Trends and Hotspots to Optimize Resources. Public-private partnerships have formed to make big data sets publicly available for stakeholders to analyze. The idea behind this access is that a single entity or closed ecosystem may not be able to quickly develop the analytical tools to derive relevant and accurate insights from all the data available to us around COVID-19. This is an inherent challenge—and value—of big data sets, and open access is critical when time is of the essence. For example, GitHub

[1] Johns Hopkins Univ., GitHub, Interactive Dashboard, *available at* https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6 (last visited Apr. 7, 2020).

and Johns Hopkins University partnered to create a dashboard of coronavirus infection data, pulled from a wide variety of public and private sources.[2] The centralizing of all this relevant data, even when it is unstructured and messy, could yield important insights into the spread of the virus.

By scouring "foreign-language news reports, animal and plant disease networks, and official proclamations," artificial intelligence (AI) company BlueDot's algorithm flagged the outbreak—which BlueDot then outlined in a report sent to clients—nine days before the World Health Organization (WHO) released its first COVID-19 statement.[3] Later on in the spread of COVID-19, fellow witness Kinsa Health began publishing anonymous temperature data from its smart thermometer, revealing valuable insights about infection patterns.[4] Kinsa adapted an analytics tool it usually uses to track the spread of influenza to detect instances of "atypical fever," a characteristic of COVID-19 infection. Notably, the U.S. Health Weather Map Kinsa created with this data showed how effective stay-at-home orders are in immediately stemming the infection rate.

Similarly, the HealthMap team at CHI Steering Committee Member Boston Children's Hospital created the COVID Near You map to help track the spread of the disease. The data is based on a simple survey asking whether a participant has had a flu vaccine and whether they feel well or sick.[5] Even this incredibly simple input can produce valuable insights when put together with a large data set and visualized on a map. These examples are illustrative of how the effective use of big data can help public health officials, providers, and the general public better understand a fast-evolving, global pandemic. But it also illustrates that big data insights are a piece of a much larger puzzle.

The question for policymakers is, "how should the findings from big data be put to use?" The trends BlueDot and Kinsa identify need to be verified against other data and weighed against a shifting set of considerations, ultimately considered by a human being. A sluggish response to an approaching crisis can be deadly, but policymakers justifiably want to avoid overreacting if the early warning ends up being a false alarm as events unfold. We observed a variety of data-driven policy responses to COVID-19. On one end is Taiwan's, which involves the overlay of patient data from the national insurance database with passport history, to identify people who recently traveled to high-risk areas.[6] Then, the Taiwanese government actively monitored the precise

---

[2] Johns Hopkins Univ., GitHub, Interactive Dashboard, *available at* https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6 (last visited Apr. 7, 2020).
[3] Eric Niiler, "An AI Epidemiologist Sent the First Warnings of the Wuhan Virus," WIRED (Jan. 25, 2020), *available at* https://www.wired.com/story/ai-epidemiologist-wuhan-public-health-warnings/.
[4] Donald G. McNeil, Jr., "Restrictions are Slowing Coronavirus Infections, New Data Suggest," THE NEW YORK TIMES (Mar. 30, 2020), *available at* https://www.nytimes.com/2020/03/30/health/coronavirus-restrictions-fevers.html; KINSA INSIGHTS, US HEALTH WEATHER MAP, *available at* https://healthweather.us/?mode=Atypical.
[5] Nancy Fliesler, "Crowdsourcing the COVID-19 pandemic in real time," Discoveries: Stories and news from Boston Children's (Mar. 26, 2020), *available at* https://discoveries.childrenshospital.org/covid-near-you-coronavirus-tracking/.
[6] Jason Wang, MD, PhD, et al, "Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing," JAMA NETWORK (Mar. 3, 2020), *available at* https://jamanetwork.com/journals/jama/fullarticle/2762689.

location of those identified as high risk using mobile phone data to enforce mandatory home quarantines.

In responses like Taiwan's, the availability of high-quality and complete data sets helped enable a policy response that effectively stopped the spread of COVID-19. However, the ready availability of an extraordinarily complete picture about individuals' movements to a government authority is not generally a feature of American policy, which tends to avoid such invasive surveillance and enforcement without due process. And yet, on the other end of the policy response spectrum, Italy did little to address the spread of the virus until infections had overtaken its healthcare system, ultimately resulting in a nationwide stay-at-home order and the shuttering of non-essential business.[7] With the judgment call rightfully in the hands of those who are politically accountable, the task before us is to ensure big data sets are at policymakers' (and the broader healthcare ecosystem's) disposal, consistent with privacy and other important public policy considerations.

Helping Develop Treatments and a Vaccine. The White House partnered with several stakeholders to produce the COVID-19 Open Resource Dataset Challenge (CORD-19),[8] calling on researchers to draw insights from a large dataset. The Challenge encourages stakeholders to develop AI-driven algorithms to sift through a collection of 47,000 extraordinarily dense academic research articles on COVID-19 and related coronaviruses. It may come as a surprise that simply distilling salient pieces of academic literature requires big data tactics, but the sheer volume of medical publications researchers produce each month is staggering. Especially useful are those algorithms that can process natural language looking for specific, self-taught trends or identifiers. Relatedly, researchers are also using AI to suggest components of a vaccine "by understanding viral protein structures."[9] AI algorithms have proven effective at determining the actual shape of a virus's protein structure, which in turn helps with the development of certain kinds of vaccines.

III. Big Data Privacy Concerns in the Coronavirus Crisis

Creating and Using Big Data Sets Consistent with Privacy Expectations. Beyond the Taiwan example described above, other nations are engaging in their own versions of highly targeted surveillance. Israel is tracking citizens' movements using smartphone location data and even sending text messages to people who were recently near a

[7] Gary P. Pisano, Raffaela Sadun, and Michele Zanini, "Lessons from Italy's Response to Coronavirus," HARVARD BUS. REV. (Mar. 27, 2020), *available at* https://hbr.org/2020/03/lessons-from-italys-response-to-coronavirus.
[8] COVID-19 Open Research Dataset Challenge, https://www.kaggle.com/allen-institute-for-ai/CORD-19-research-challenge (last visited Apr. 7, 2020).
[9] Oren Etzioni and Nicole Decario, "AI Can Help Scientists Find a Covid-19 Vaccine," WIRED (Mar. 28, 2020), *available at* https://www.wired.com/story/opinion-ai-can-help-find-scientists-find-a-covid-19-vaccine/.

person known to have been infected with COVID-19, with an order to self-quarantine.[10] While Israeli courts blocked the use of this data to enforce quarantines,[11] even the use of it to send unsolicited text messages and swiftly apply impromptu quarantines raises some questions.

By contrast, in the United States, private companies are leading the charge on big data sets about location, with persistent privacy oversight by policymakers. For example, Google is producing reports on foot traffic patterns using smartphone location data.[12] However, there are limitations to the reports because they only use high-level data indicating a percentage decrease or increase in foot traffic in six different types of locations (e.g., workplaces, retail, and recreation sites) over a given period of time.[13] Their vagueness is in part the result of federal and state privacy law, which generally prohibit deceptive practices, including the disclosure of private data in a manner that is inconsistent with a company's own privacy policies or where the individual never consented to the disclosure. News articles variously describe these kinds of high-level reports as tracking compliance with stay-at-home orders, but they only do so in an indirect sense and certainly not to the degree to which Taiwan or Israel track compliance, which involves the use of individual location data.

The availability of high-level reports like the ones Google produces are useful, but the federal government is already looking into more granular data to implement more targeted stay-at-home or other social distancing measures. For example, Massachusetts Institute of Technology (MIT) researchers are developing a tool, the Private Kit app, to anonymously track both COVID-19 positive patients and those who have not tested positive.[14] The idea is to provide contact tracing capabilities, which involve 1) identifying individuals who are infected (contact identification); 2) contact listing; and 3) contact follow-up.[15] Israel and Taiwan perform these functions with a high degree of accuracy, but the process need not involve the enforcement measures that accompany it in those countries. In fact, experts have said that such measures are unlikely to help much in parts of the United States like New York, as infection rates have gone uncontrolled in those areas and progressed beyond the point where targeted measures can help. But there may yet be an opportunity to leverage location tracking in other parts of the nation in order to save human lives.

In another example, developers rapidly produced consumer screening and information apps. Apple developed its COVID-19 app in partnership with the White House Coronavirus Task Force, the CDC, and HHS to provide actionable information directly to

---

[10] Daniel Estrin, "Israel Begins Tracking and Texting Those Possibly Exposed to Coronavirus," NPR (Mar. 19, 2020), *available at* https://www.npr.org/2020/03/19/818327945/israel-begins-tracking-and-texting-those-possibly-exposed-to-the-coronavirus.
[11] *Id.*
[12] Steve Overly, "Google wielding its vast troves of phone-tracking data in virus fight," Politico (Apr. 3, 2020), *available at* https://www.politico.com/news/2020/04/03/google-coronavirus-tracking-162715.
[13] *See, e.g.,* COVID-19 Community Mobility Report, Virginia (Mar. 29, 2020), *available at* https://www.gstatic.com/covid19/mobility/2020-03-29_US_Virginia_Mobility_Report_en.pdf.
[14] Douglas Belkin and Kirsten Grind, "MIT Researchers Launch Location-Tracking Effort for New Coronavirus," The Wall St. J. (Mar. 27, 2020), *available at* https://www.wsj.com/articles/mit-researchers-launch-location-tracking-effort-for-the-new-coronavirus-11585315674?mod=article_inline.
[15] WORLD HEALTH ORG., CONTACT TRACING (May 2017), *available at* https://www.who.int/features/qa/contact-tracing/en/?mod=article_inline.

consumers in an easy-to-use format. The app prompts users to answer a series of questions either about themselves or a loved one around risk factors, including whether they have been exposed to the virus and their symptoms.[16] Notably, the app does not require the user to log in (so the user's answers are not associated with a specific Apple ID), nor does it collect any personal data or send any personal information back to Apple or any other third parties.[17] This provision of up-to-date guidance information in an evolving scenario like the COVID-19 pandemic, tailored to the user's needs, is a great example of a public-private partnership to inform consumers and position them to address the risks. App Association member Rimidi also provides a COVID-19 screening tool, but the Rimidi app's end users are providers.[18] The app helps healthcare systems screen patients so that they can make informed care decisions and optimize resources to where there is the most urgent need.

With Location Data, Privacy is Possible. Ideally, federal, state, and local governments could enact targeted measures that significantly stem the spread of COVID-19 in high-risk areas and at high-risk times, while enabling certain parts of the economy to open back up where there is mitigation of risk—all with *anonymous* data. The Private Kit app takes privacy protective steps that may help provide both actionable data and effective anonymity. For example, when a user downloads the app, it clarifies that location data stays on the user's phone and does not go to a centralized server. Instead, when turned on, the app tracks the user's location and stores it in an encrypted format—which it apparently sends, again encrypted, directly to other phones when queried. Theoretically, it would be difficult for any single user of the app to discern the identity of the person signified by one of the dots on the map. The problem Private Kit encounters is whether enough people will download this app quickly enough for it to be useful for policymakers and users. Similar ideas, like NextTrace have also cropped up, but the effectiveness of these tools may be limited if a single, popular choice does not soon emerge.

The Private Kit example is reminiscent of some of the privacy measures large tech platforms are using to protect privacy in the smart device space—techniques that could prove useful in the COVID-19 response. One challenging task before experts is how to train algorithms without collecting and centralizing large volumes of personally identifiable information. Smartphone makers met this challenge by employing federated learning to train voice recognition algorithms. Under this process, the only voice that directly trains the voice recognition model installed natively on a certain smartphone is that of the owner. Nobody else's personally identifiable data uploads directly to that copy of the model, nor is personal data uploaded to a server. Instead, the updated version of the voice recognition model (as trained by a given iPhone owner) is sent to the cloud, where it updates the collective model—which is in turn pushed to everyone's

[16] CENTERS FOR DISEASE CONTROL AND PREVENTION, "CDC Statement on COVID-19 Apple App," Press Release (Mar. 27, 2020), *available at* https://www.cdc.gov/media/releases/2020/s0327-statement-covid-19-apple-app.html.
[17] *See* Michael Potuck, "US Senators are asking Apple how private their COVID-19 app is, so we tested it," 9TO5MAC (Apr. 3, 2020), *available at* https://9to5mac.com/2020/04/03/us-senators-are-asking-apple-how-private-their-covid-19-app-is-so-we-tested-it/.
[18] RIMIDI, "Rimidi Unveils New App to Accelerate Patient Screenings for COVID-19," Press Release (Mar. 6, 2020), *available at* https://rimidi.com/news/rimidi-unveils-new-app-to-accelerate-patient-screenings-for-covid-19.

device.[19] Add to this a layer of differential privacy—where random data or "noise" is added to the model before encryption of personal data, and individual contributions by a given user are limited—and retracing the model's steps to identify a single person's voice data is extremely difficult.[20] Meanwhile, the model itself is trained with widely distributed, high-quality data. With methods like these, we can realize the benefits of big data analytics while minimizing privacy risks.

The COVID-19 Pandemic Underscores the Need for a National Privacy Law. National privacy legislation should ensure companies are using default privacy measures like those described above. Animating some of the privacy concerns policymakers have expressed about the use of big data to address the COVID-19 pandemic is a (not entirely unfair) lack of trust in how tech-driven companies are using sensitive personal data, especially location data.[21] While many of us worry that governmental intrusions to address the COVID-19 pandemic would be difficult to pull back, policymakers also worry that corporate surveillance efforts could later turn into unexpected uses of sensitive data and exposure to additional risk of unauthorized access. The passage of a strong, national privacy framework could help alleviate the stated concerns with private sector use of data.

The sudden necessity of harnessing big data to create effective—and privacy protective—tracking tools shines a light on the absence of a federal privacy regime that mandates a baseline of privacy protective measures as a default. The Federal Trade Commission has long encouraged American companies to use "privacy by design," whereby companies develop products and services with privacy as a central focus from the ground up.[22] Likewise, a federal law should require companies to build products and services with the assumption that consumers are privacy protective by nature and do not wish to spend their days parsing privacy policies to make key privacy-related choices. Similarly, a federal law should empower consumers with rights like those that appear in the General Data Protection Regulation (GDPR). Limited rights to delete, correct, and access personal data from a covered company would go some distance toward restoring trust in the use of personal data. The shared attributes of the proposals the Chairman and Ranking Member of this committee should be noted in this regard and your work toward a compromise bill strongly commended.[23] A single, national set of rules would be especially important for small companies like App Association members to avoid confusion, especially as the development and iteration of software needs to be quick to address a crisis like COVID-19. The absence of a federal privacy framework

[19] Karen Hao, "How Apple personalizes Siri without hoovering up your data," MIT TECH. REV. (Dec. 11, 2019), *available at* https://www.technologyreview.com/s/614900/apple-ai-personalizes-siri-federated-learning/.
[20] APPLE, DIFFERENTIAL PRIVACY, *available at* https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf.
[21] *See, e.g.,* Alfred Ng, "COVID-19 tracking efforts pose a privacy risk, Senator says," C|NET (Mar. 19, 2020), *available at* https://www.cnet.com/news/covid-19-tracking-efforts-pose-a-privacy-risk-senator-says/.
[22] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012), *available at* https://www.ftc.gov/public-statements/2012/06/privacy-design-and-new-privacy-framework-us-federal-trade-commission.
[23] *See, e.g.,* Graham Dufault, "This Actually was Kind of the Year of Privacy, and Other Thoughts," ACT | THE APP ASSOCIATION BLOG (Dec. 19, 2020), *available at* https://actonline.org/2019/12/19/this-actually-was-kind-of-the-year-of-privacy-and-other-thoughts/.

has left us less prepared to respond to the crisis with a coordinated, data-driven, and trusted effort. We should avoid making the same mistake in the future.

IV. Policymakers Should Make Digital Health Tools and Data More Accessible, While Protecting Privacy

Healthcare Data Remains Siloed. Through CHI, we advocate for patients to be able to share their healthcare data with digital health companies that can help them make use of it. But in general, electronic health records (EHR) companies decline to transfer that data except inside their own network of providers and business associates (BAs), citing Health Insurance Portability and Accountability Act (HIPAA) compliance concerns. The problem with this, of course, is that HIPAA is supposed to make data portable, as the name suggests. And EHRs have emerged as a chokepoint for healthcare data that patients should otherwise be able to use as they wish.

Besides harming big data competencies, outdated healthcare policies have also directly harmed patients. It would be a great tragedy if we yanked telehealth and remote physiologic monitoring (RPM) away from patients just as the general public begins to realize their potential. Certainly, the ability to rely on telehealth (defined in Medicare as live voice or video visits between patients and caregivers) is a sudden necessity during the pandemic as caregivers must screen and monitor patients from a distance. Avoiding such basic communications technologies because of fraud or abuse concerns when public health demands patients stay at home would be nothing short of a catastrophic win for red tape. What surprises many of us, however, is just how unprepared our relative inability to make use of digital health has made us for pandemics like COVID-19.

Federal healthcare policy has generally failed to keep up with modern technologies, preventing mobile software and even the use of telephonic communications from beneficial use in a healthcare setting. In turn, these policy features restrained the accumulation and analytical potential of big data for healthcare, including the COVID-19 pandemic. The bureaucratic obstacles around simply discussing your health with a physician on the phone revealed themselves in terrifying detail, but fortunately, policymakers responded decisively. In its series of COVID-19 response packages, most recently with the Coronavirus Aid, Recovery, and Economic Security (CARES) Act, Congress made unprecedented policy changes to enable the use of telehealth and even digital health tools like RPM for Medicare patients.[24] The Department of Health and Human Services (HHS) also made several fundamental policy changes (mostly through guidance) to enable the use of RPM and telehealth, consistent with the new statutory

[24] *See* CORONAVIRUS AID, RELIEF, AND ECONOMIC SECURITY (CARES) ACT, Sec. 3701 *et seq.* (H.R. 748, 116th Cong.).

changes.[25] However, many of those changes lapse at the end of the Public Health Emergency associated with COVID-19. This is a problem for big data-enabled tools.

That telehealth and RPM are efficient and effective tools for patients and providers is demonstrable. From saving Medicaid budgets hundreds of millions to helping diabetes patients lower their A1C to controlled levels, telehealth and RPM are showing that they can save money and produce better outcomes for patients.[26] Unfortunately, the available data suggests that *almost all* of the Americans who die of COVID-19 had at least one underlying or chronic condition—and 78 percent of COVID-19 patients who necessitated a visit to the intensive care unit (ICU) had at least one chronic condition.[27] Again, these are patients for whom RPM and telehealth could augment an already-strained healthcare system to provide them the monitoring and management they needed to control their chronic issues. Not only that, they are patients for whom quick access to records and assistance from big data analytics could mean life or death. Clinical decision support and screening tools like Rimidi's are currently helping healthcare systems triage patients who are less likely to need immediate care so that resources can be directed to those most in need. This function is even more critical during the crisis, when resources must focus on patients presenting the highest risks, while closely monitoring relatively lower-risk patients remotely. Access to patient data is a critical component of making these big data-driven tools work, because a patient's history can be integral to understanding the risks to which the patient is exposed.

This need for data access led App Association member Particle Health to create a platform that navigates the current, byzantine management of healthcare data to make data more usable for patients, providers and researchers. Particle's platform seeks to carry out a similar function to Plaid, credited with enabling financial services innovations like Venmo by handling secure back-end access to sensitive banking data. Likewise, Particle provides patients with their own healthcare data in a format that third-party digital health companies can use as the patient directs, including allowing the use of data in larger data sets. The access network Particle Health cobbled together is impressive, including key healthcare data on 250 million lives.[28] In fact, Particle's founder has said he would welcome the ability to provide limited data access to the Centers for Disease Control and Prevention (CDC), except that the EHR companies from which Particle provides access have thus far denied this request. Bulk access to healthcare data for legitimate and secure uses through an application programming interface (API) is a critical element of being able to address a pandemic like COVID-19 through the use of big data. This is why CHI supported HHS' recent final rules, requiring

---

[25] Connected Health Initiative, COVID-19 & Digital Health (2020), *available at* https://static1.squarespace.com/static/57ed48b4f5e23125aa094623/t/5e838c3c23739d573b12f213/1585679423005/COVID-19+Digital+Health+Policy+Primer+%28033120%29.pdf.

[26] "Healthcare in Rural America: Examining Experiences and Costs," Roundtable Hearing, U.S. Senate Committee on Health, Education, Labor, and Pensions (HELP), Subcommittee on Primary Health and Retirement Security, 115th Cong. (Sep. 25, 2018) (Statement of Morgan Reed, Executive Director, Connected Health Initiative), *available at* https://actonline.org/wp-content/uploads/CHI-Testimony-Health-Care-in-Rural-America.pdf.

[27] Centers for Disease Control and Prevention, Morbidity and Mortality Weekly Report (Apr. 3, 2020), *available at* https://www.cdc.gov/mmwr/volumes/69/wr/pdfs/mm6913-H.pdf.

[28] Logan Plaster, "Particle Health's API makes COVID-19 screenings faster and smarter, and now it's free to use," STARTUP HEALTH BLOG (Mar. 17, 2020), *available at* https://healthtransformer.co/particle-healths-api-makes-covid-19-screenings-faster-and-smarter-and-now-it-s-free-to-use-d377d492ddae.

EHRs to honor patient requests to transfer their own healthcare data to a third party, subject to a variety of restraints and caveats.[29] However, although the rules delay enforcement with a two-year phase-in, the implementation of the rules should occur as soon as practicable. If they had been implemented several years ago, we would have been in a better position to respond to the crisis armed with big data tools. The COVID-19 pandemic has only intensified the need for patients to be able to access their own health data as soon as possible, especially for those who are at risk and need their health histories to help providers understand the patient's level of exposure risk.

Live Video and Telephonic Visits are a Necessity. Broadband-enabled or telephonic communications with caregivers can automatically produce valuable, reliable data in a manner that is more accurate (not to mention *far* less time-consuming for physicians) than manual entry by caregivers. This is true even if the only kind of data collected around an interaction is metadata—that information can still be valuable, if the patient asks for analysis. But it should be up to the patient to determine collection and use of their data. The COVID-19 pandemic is revealing the utility of end-to-end encrypted tools like FaceTime—which shields the content of live conversations from anyone besides the physician and patient—in the healthcare setting. The recording of the confidential conversation can still be put to beneficial use consistent with a patient's desires and expectations without unauthorized entities accessing it.

Recognizing patient preferences, HHS recently issued guidance indicating that it would not enforce the HIPAA requirement for companies that provide such end-to-end encrypted communications apps to enter into BA agreements with the healthcare provider serving a given patient. This is an important clarification, but more permanent guidance is necessary to account for the nature of end-to-end encrypted services beyond the COVID-19 public health emergency. To this end, HHS's Office of Civil Rights should provide guidance clarifying that certain end-to-end encrypted apps are "conduits" under HIPAA, thus dispensing with the requirement to forge a superfluous BA between the app maker and the healthcare provider. Specifically, the guidance should clarify that some storage of call related metadata counts as "random or infrequent," so long as that information is being used to support the service and the storage is for a period of time necessary to support the service. This is consistent with the preamble to a recent HIPAA rule, which states, "entities that act as mere conduits for the transport of protected health information but do not access the information other than on a *random or infrequent* basis are not business associates."[30] This clarity would enable patients and providers to rely on highly secure means of communication without putting all parties through unnecessary red tape.

---

[29] *See* Brian Scarpelli, "Connected Health Initiative Applauds New ONC and CMS Rules on Interoperability and Information Blocking," CONNECTED HEALTH INITIATIVE BLOG (Mar. 9, 2020), *available at* http://www.connectedhi.com/blog/2020/3/9/connected-health-initiative-applauds-new-onc-and-cms-rules-on-interoperability-and-information-blocking.

[30] 78 Fed. Reg. 5566, 5571 (Jan. 25, 2013), *available at* https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

V. Conclusion

We sincerely appreciate the opportunity to provide testimony in this paper hearing. Across all of the various ways in which stakeholders are leveraging big data and digital tools to produce actionable insights to combat the novel coronavirus, a theme emerges that there are privacy protective ways of handling potentially sensitive data. Moreover, we are able to see the experiences of other countries around the globe, which means we can learn from them. But it also means the ability to leverage data is a global policy problem. As a corollary, data protection tools like strong encryption emerge as crucially important as we develop new ways of manipulating data, combining sources, and training models. Efforts that weaken encryption in favor of governmental access may seem attractive during public health emergencies or to combat certain criminal activities, but they would do serious damage to our ability to harness big data while protecting privacy. We look forward to assisting with the Committee's work as it examines the use of big data, including how such uses affect privacy and in the development of bipartisan consumer privacy legislation.

Appendix: Resources from App Association Members and the Broader App Ecosystem

In this unprecedented time, our global community is facing a unique set of pressures to find balance and stillness in a turbulent environment. As we seek out new ways to communicate, work, monitor our health and wellness, and have fun, the innovative minds of ACT| The App Association members have been working hard.

Our members are working hard on the front lines to provide telehealth support and resources, offering their services and expertise to businesses that need to pivot to a digital presence, and are creating innovative solutions to empower other local small businesses in their area. Below is a small example of what our member companies are doing to help during the COVID-19 pandemic.

AirTies

Turkey-based AirTies provides in-home WiFi solutions, developing both software and hardware, that allow users to enjoy increased wireless speeds and coverage throughout their homes and offices. Founded in 2004, the products of this medium-sized company have already been installed in over 25 million homes and some of AirTies's biggest customers include AT&T, Singtel, and Sky. If you are now working from home due to COVID-19, it is imperative that your WiFi is working, and AirTies's solutions can extend your WiFi's range and help optimize its performance.

Andaman7

Andaman7 is a Belgian eHealth company with an app that is designed to close the information management gap in the health sector and to facilitate communication between medical professionals and patients. Andaman7 empowers users to take control of their own, or a dependent's, health data by allowing patients to collect and enter all their health data and store it in one place. Patients can choose to share their data with medical professionals to facilitate remote patient monitoring. All health data is stored on the user's device, to guarantee privacy. Recently, Andaman7 launched a special in-app COVID-19 feature that helps with informing patients, triage and self-testing, data collection for crisis management, and medical research.

Beyond Lucid Technologies

Located in Concord, California, and founded in 2009, Beyond Lucid Technologies is a health and safety IT firm that builds software to help first responders do their job safer and more efficiently. Their platform uses telemedicine, GPS, and other technology to help health systems run more effectively. Beyond Lucid has added COVID-19 elements to its fire and EMS data platform give institutions and public health agencies a chance for heads-up preparation, without requiring field crews to change their behavior.

Bluestream Health

Located in New York City, Bluestream Health created a virtual care platform where patients are able to receive remote and video assistance at the point of care across many disciplines. They provide access to specialists and have the ability to interpret 200 languages, including American Sign Language, to ensure that patients can access care when and how they need it. Bluestream Health is providing a free, HIPAA-compliant virtual care solution to help care providers work with patients who are impacted by the COVID-19 outbreak.

Canned Spinach

Canned Spinach, located in Cincinnati, Ohio, is a full-service design and development firm that specializes in user experience and user interface design. They were founded in 2016, and their client roster includes well-known entities like DJ Khaled and Toyota, as well as small businesses like Speakeasy and This & They. To help other small businesses during the COVID-19 pandemic, Canned Spinach created the “Stay in Cincy” database to connect Cincinnati businesses to local customers with daily offers.

Efelya

An online self-assessment platform, the French eHealth company Efelya helps women to evaluate potential risks that are specific to their pregnancies. Efelya uses medical algorithms and data analytics to create a “pregnancy passport” and customized notifications for its users. Users can also share their records with their doctors, which can help to identify potential problems earlier and minimize pregnancy risks overall. Efelya’s pregnancy passport can save women and their doctors valuable time by helping to triage symptoms, and in case of an emergency, keep pregnant women out of hospitals, especially those with a high number of COVID-19 patients, when possible.

Particle Health

Founded in 2017 and located in New York City, Particle Health works with data networks to better facilitate data sharing via APIs, ensuring that patients have their data when they need it. They currently have the ability to help more than 250 million patients access their data and is making its API for electronic medical records free to organizations and platforms screening for COVID-19.

Rimidi

Rimidi creates mobile apps that work directly within electronic health records (EHR) to combine patient-generated health data with clinical data, allowing for patient-specific clinical insights. They have developed a COVID-19 screening application based on the widely accepted Fast Healthcare Interoperability Resources (FHIR) standard for health systems to identify and flag at-risk patients via survey prior to existing appointments. Their tool enables health systems to mitigate the spread of COVID-19, as well as optimize treatment.

As mentioned above, the companies we've listed here are just a few examples of the work our members are doing to help during this time. Not only have we compiled a list of members and the work they're doing, but we have also assembled a list of resources to help and empower our members. This includes resources from the Small Business Administration (SBA) and the Federal Communications Commission (FCC) to letters and filings our Connected Health Initiative (CHI) has championed. For more information on these resources, please follow the links below.

https://actonline.org/covid-19-resources/
http://www.connectedhi.com/covid19