Technology Policy Update
10 April 2020
By Michael Kans, Esq.

"Paper" Hearing on COVID-19 and Big Data

In a novel format, a committee poses questions to experts about the use of big data in the fight to control COVID-19. Witnesses have eight business days to respond. However their written testimony makes clear their concerns on the use of location data and other data to track possible transmission of the respiratory illness.

On April 9, the Senate Commerce, Science, and Transportation Committee held a virtual hearing of sorts as all the proceedings would occur through the written word with the chair, ranking member, and witnesses all submitting statements. Then all the members were to submit written questions to the witnesses who will have 96 business hours to respond or what appears to be 12 days. The questions posed to each witness by each member of the committee have been posted on the hearing webpage as well.

In his written statement, Chair Roger Wicker (R-MS) stated "[a]s the public and private sectors race to develop a vaccine for [COVID-19], government officials and health-care professionals have turned to what is known as "big data" to help fight the global pandemic." He stated "[i]n recognition of the value of big data, Congress recently authorized the CDC, through the bipartisan coronavirus relief package, to develop a modern data surveillance and analytics system," a reference to the $500 million appropriated for "for public health data surveillance and analytics infrastructure modernization." Wicker said "[t]his system is expected to use public health data inputs – including big data – to track the coronavirus more effectively and reduce its spread." He added "[s]tate governments are also using big data to monitor the availability of hospital resources and manage supply chains for the distribution of masks and other personal protective medical equipment."

Wicker remarked,

- Recent media reports revealed that big data is being used by the mobile advertising industry and technology companies in the United States to track the spread of the virus through the collection of consumer location data. This location data is purported to be in aggregate form and anonymized so that it does not contain consumers' personally identifiable information. It is intended to help researchers identify where large crowds are forming and pinpoint the source of potential outbreaks. The data may also help predict trends in the transmission of COVID-19 and serve as an early warning system for individuals to self-isolate or quarantine.
- In addition to these uses, consumer location data is being analyzed to help track the effectiveness of social distancing and stay-at-home guidelines. Data scientists are also seeking ways to combine artificial intelligence and machine learning technologies with big data to build upon efforts to track patterns, make diagnoses, and identify other environmental or geographic factors affecting the rate of disease transmission.
- The European Union is turning to big data to stop the spread of the illness as well. Italy, Germany, and others have sought to obtain consumer location data from telecommunications companies to track COVID-19. To protect consumer privacy, EU member states have

> committed to using only anonymized and aggregate mobile phone location data. Although the EU's General Data Protection Regulation does not apply to anonymized data, EU officials have committed to deleting the data once the public health crisis is over.

Wicker asserted, "[t]he potential benefits of big data to help contain the virus and limit future outbreaks could be significant." He stated "[r]educing privacy risks begins with understanding how consumers' location data – and any other information – is being collected when tracking compliance with social distancing measures." He contended that "[e]qually important is understanding how that data is anonymized to remove all personally identifiable information and prevent individuals from being re-identified…[and] I look forward to hearing from our witnesses about how consumer privacy can be protected at every stage of the data collection process."

Wicker stated, "I also look forward to exploring how consumers are notified about the collection of their location information and their ability to control or opt out of this data collection if desired." He explained "[g]iven the sensitivity of geolocation data, increased transparency into these practices will help protect consumers from data misuse and other unwanted or unexpected data processing." Wicker added "I hope to learn more about how location data is being publicly disclosed, with whom it is being shared, and what will be done with any identifiable data at the end of this global pandemic."

Wicker concluded,

> Strengthening consumer data privacy through the development of a strong and bipartisan federal data privacy law has been a priority for this Committee. The collection of consumer location data to track the coronavirus, although well intentioned and possibly necessary at this time, further underscores the need for uniform, national privacy legislation. Such a law would provide all Americans with more transparency, choice, and control over their data, as well as ways to keep businesses more accountable to consumers when they seek to use their data for unexpected purposes. It would also provide certainty and clear, workable rules of the road for businesses in all 50 states, and preserve Americans' trust and confidence that their data will be protected and secure no matter where they live.

Ranking Member Maria Cantwell (D-WA) asserted, "[r]ight now, we must ensure there are enough hospital beds, enough personal protective equipment, and enough ventilators and medical supplies to withstand the full force of this virus as it peaks in communities across our country" in her opening statement. She stated, "[w]e need robust testing, and as the virus finally fades, we'll need to deploy contact tracing systems so that we can respond quickly to outbreaks and stamp it out for good." Cantwell claimed, "[d]ata provides incredible insights that can assist us in these efforts, and we should be doing everything possible to harness information in a manner that upholds our values." She remarked, "[t]o gain and keep the public's trust about the use of data, a defined framework should be maintained to protect privacy rights…[that] at a minimum, should ensure that information is used:

(1) for a specific limited purpose, with a measurable outcome and an end date,
(2) in a fully transparent manner with strong consumer rights, and
(3) under strict accountability measures.

Cantwell stated, "[w]e must always focus on exactly how we expect technology to help, and how to use data strategically to these ends…[and] [w]e must resist hasty decisions that will sweep up massive, unrelated data sets." She further argued, "we must guard against vaguely defined and

non-transparent government initiatives with our personal data…[b]ecause rights and data surrendered temporarily during an emergency can become very difficult to get back."

Cantwell expressed her belief that "there are three advantages to data that need to be harnessed at this time: the power to predict, the power to discover, and the power to persuade." She remarked, "[d]ata helps us build models based on what has come before…[and] [w]e can use these models to identify patterns to help us prepare for what might be next, whether those are predictions of where disease is spreading, estimations of community needs, or coordination of scarce resources." Cantwell said, "[l]arge publically available data sets also help us identify patterns and solutions that cannot be seen with a more fragmented, less complete picture." She asserted, "[d]iscoveries and insights that once were hidden can now be brought to light with the help of advanced data analysis techniques." She said, "[a]nd when there are vital messages to share, data allows us to get those messages out to everyone who needs to hear them…[and] [m]essages about social distancing, exposure risks, and treatment options are just a few of the many types of essential communications that can be informed and enhanced by data analysis."

Cantwell summed up:

- The world is now confronting a challenge of tremendous urgency and magnitude. At some point, we will be opening up our society and our economy again. First, we're going to need robust testing. And when that time comes, we're also going to need technology, powered by data, to help us safely transition back to a more normal way of life.
- Our job in Congress is to help provide the tools needed to turn back this disease, and to understand how we marshal innovation and technology in a responsible way to respond to this challenge, both in the short term and for what we are starting to understand may be a very long fight ahead.
- We are only at the beginning of this fight. We urgently need to plan for the days and, yes, the years ahead; we must discover, test, and distribute new cures faster than ever before; we need our greatest minds, wherever they may be, to collaborate and work together; and we must build unity because ultimately, that is our greatest strength.

University of Washington Professor of Law Ryan Calo explained

> In this testimony, I will address some of the ways people and institutions propose to use data analytics and other technology to respond to coronavirus. The first set of examples involves gaining a better understanding of the virus and its effects on American life. By and large I support these efforts; the value proposition is clear and the privacy harms less pronounced. The second set of examples involves the attempt to track the spread of COVID-19 at an individual level using mobile software applications ("apps"). I am more skeptical of this approach as I fear that it threatens privacy and civil liberties while doing little to address the pandemic. Finally, I conclude with the recommendation that, however we leverage data to fight this pandemic, policymakers limit use cases to the emergency itself, and not permit mission creep or downstream secondary uses that surprise the consumer.

Calo said

> I am not opposed to leveraging every tool in our technical arsenal to address the current pandemic. We are facing a near unprecedented global crisis. I note in conclusion that there will be measures that are appropriate in this context, but not beyond it. Americans and their representatives should be vigilant that whatever techniques we use today to combat

> coronavirus do not wind up being used tomorrow to address other behaviors or achieve other goals. To paraphrase the late Justice Robert Jackson, a problem with emergency powers is that they tend to kindle emergencies.

Calo asserted

> In national security, critics speak in terms of mission creep, as when vast surveillance powers conferred to fight terrorism end up being used to enforce against narcotics trafficking or unlawful immigration. In consumer privacy, much thought is given to the prospect of secondary use, i.e., the possibility that data collected for one purpose will be used by a company to effectuate a second, more questionable purpose without asking the data subject for additional permissions. No consumer would or should expect that the absence of certain antibodies in their blood, gathered for the purpose of tracing a lethal disease, could lead to higher health insurance premiums down the line. There is also a simpler danger that Americans will become acclimated to more invasive surveillance partnerships between industry and government.14My hope is that policymakers will expressly ensure that any accommodations privacy must concede to the pandemic will not outlive the crisis.

ACT | The App Association Senior Director for Public Policy Graham Dufault explained some of the big data privacy concerns in the COVID-19 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 4person known to have been infected with COVID-19, with an order to self-quarantine.10While Israeli courts blocked the use of this data to enforce quarantines,11even 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.12However, 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.13Their 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.
- 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 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.21While 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.
- Healthcare Data Remains Siloed. Through the Connected Health Initiative (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.

Interactive Advertising Bureau Executive Vice President for Public Policy Dave Grimaldi stated

> While self-regulation has been a useful mechanism to encourage responsible data use, federal leadership is now needed to ensure that robust consumer privacy protections apply consistently throughout the country. The time is right for the creation of a new paradigm for data privacy in the United States. To this end, IAB is a key supporter of Privacy for America, a broad industry coalition of top trade organizations and companies representing a wide cross-section of the American economy that advocates for federal omnibus privacy legislation. Privacy for America has released a detailed policy framework to provide members of Congress with a new option to consider as they develop data privacy legislation for the United States. Participants in Privacy for America have met with leaders of Congress, the FTC, the Department of Commerce, the White House, and other key stakeholders to discuss the ways the framework protects consumers while also ensuring that beneficial uses of data can continue to provide vast benefits to the economy and mankind.

Grimaldi claimed

The Privacy for America framework would prohibit, rather than allow consent for, a range of practices that make personal data vulnerable to misuse. Many of these prohibitions would apply not only to companies that engage in these harmful practices directly, but to suppliers of data who have reason to know that the personal information will be used for these purposes.

- **Eligibility Determinations.** Determining whether individuals are eligible for benefits like a job or credit are among the most important decisions that companies make. Although many of these decisions are currently regulated by existing sectoral laws (e.g., the Fair Credit Reporting Act), companies can easily purchase data on the open market to evade compliance with these laws. Privacy for America's framework would prevent this abuse by banning the use of data to make eligibility decisions—about jobs, credit, insurance, healthcare, education, financial aid, or housing—outside these sectoral laws, thereby bolstering and clarifying the protections already in place. It also would provide new tools to regulators to cut off the suppliers of data that undermine these protections. To the extent that companies are unsure about whether a practice is permitted under existing law, they would be able to seek guidance from the FTC.
- **Discrimination.** The widespread availability of detailed personal information has increased concerns that this data will be used to discriminate against individuals. The new framework envisioned by Privacy for America would supplement existing anti-discrimination laws by banning outright a particularly pernicious form of discrimination—using data to charge higher prices for goods or services based on personal traits such race, color, religion, national origin, sexual orientation, or gender identity. As discussed below, the framework also would allow individuals to opt out of data personalization, which can contribute to discrimination.
- **Fraud and Deception.** For decades, the FTC and the states have pursued cases against companies that engage in fraud and deception. The new framework would focus specifically on the use and supply of data for these purposes. Thus, it would ban a range of fraudulent practices designed to induce the disclosure of personal information and, more generally, material misrepresentations about data privacy and security.
- **Stalking.** In recent years, the proliferation of data has made it easier to track the location and activities of individuals for use in stalking. Of note, mobile apps designed for this very purpose have been identified in the marketplace. The framework would outlaw the use of personal information for stalking or other forms of substantial harassment, and would hold these types of apps accountable.
- **Use of Sensitive Data Without Express Consent.** Consumers care most about their sensitive data, and companies should have an obligation to protect it. The new framework would prohibit companies from obtaining a range of sensitive information—including health, financial, biometric, and geolocation information, as well as call records, private emails, and device recording and photos—without obtaining consumers' express consent.
- **Special Protections for Individuals Over 12 and Under 16 (Tweens).** The Privacy for America framework includes a robust set of safeguards for data collected from tweens, an age group that needs protection but is actively engaged online and not subject to constant parental oversight. Specifically, the framework would prohibit companies from transferring tween data to third parties when they have actual knowledge of age. It also would ban payment to tweens for personal data, except under a contract to which a parent or legal guardian is a party. Finally, companies would be required to implement data eraser requirements allowing individuals to delete data posted online when they were tweens.

Center for Democracy and Technology Data and Privacy Project Director Michelle Richardson advised

When deciding what types of data practices are appropriate, Congress should remember that privacy is a balancing of equities. We no longer think of privacy as an on-off switch, or something that can be dismissed after a person agrees to a lengthy privacy policy. It instead weighs the intrusion of any product or program against the benefit of the data use, the secondary effects on individuals, and any mitigating steps that can be taken to minimize harms. As policymakers review data collection, use and sharing, they should:

- Focus on prevention and treatment, not punishment: Past epidemics have demonstrated that fear is not as effective as clear, meaningful information from a reliable source and the ability to voluntarily comply with medical and governmental directives. Successfully fighting the coronavirus will mean ensuring that a government response does not evolve into law enforcement and broad surveillance functions.
- Ensure accuracy and effectiveness: There does not appear to be a universally accepted definition of "accurate" or "effective" when it comes to predicting, preventing, or responding to the coronavirus. Nevertheless, if a tool or practice is unlikely to provide meaningful and measurable contributions to the coronavirus response, companies and governments should consider alternatives. This is not only because the privacy risks may not be justified but because people may rely on these measures in lieu of those that actually work.
- Provide actionable information: In a time of crisis, more information isn't always better. New data collection or novel data uses should inform individual, corporate, or government behavior in a constructive way. Symptom trackers, for example, may tell a person whether he or she should seek medical care. Contact tracing on the other hand, when it relies on insufficiently granular data, may result in unnecessary or unproductive quarantine, testing, and fear.
- Require corporate and government practices that respect privacy: People are reasonably fearful for their own health and the health of their loved ones. The burden for constructing privacy-protective products and responses must not be on concerned citizens but on companies and governments. That includes:
    - *A preference for aggregated data*. Individually identifiable information should not be used when less intrusive measures will suffice. If aggregated data will not do, industry best practices in anonymization and de-identification must be applied.
    - *Minimizing collection, use, and sharing*. When identifiable information is necessary, data processing should be limited when possible.
    - *Purpose limitations*. Data collected or used for the coronavirus response should not be used for secondary purposes. For corporate actors, this means advertising for commercial purposes or unrelated product development. For government actors, that means any function not directly related to their public health functions.
    - *Deletion*. Data should be deleted when it is no longer necessary for responding to the coronavirus epidemic or conducting public health research, especially if it is personally identifiable.
- Build services that serve all populations: Newly released data is confirming that minorities are contracting the coronavirus at a higher rate and are more likely to die from it.58 There are also legitimate questions about how actionable mobility tracking data is for rural, poor, and working class communities that must travel for work or to

secure food and medical care. As technology seeks to find solutions to the coronavirus, it is crucial that it does so in a way that serves all demographics and does not exacerbate existing inequalities.

- Empower individuals when possible: Epidemic response may not always allow for individualized opt-ins or opt-outs of data collection and use. To the extent possible, participation in data based programs should be voluntary and individuals should maintain traditional rights to control one's data.
- Be transparent to build trust: People will hesitate to participate in programs that involve their personal information but that are not transparent in how that information will be used. Companies that provide data, or inferences from data, and the governmental entities that use such information, must be transparent to users and residents about how data will be used.
- Be especially rigorous when considering government action: A coordinated government response is necessary for successfully fighting the coronavirus epidemic, but the United States has an important tradition of recognizing that the powers of the state pose unique threats to privacy and liberty.

DOD Revises Cybersecurity Model For Contractors; Accreditation Body Holds Webinar

The Department of Defense (DOD) issued a revised version of the Cybersecurity Maturity Model Certification (CMMC) and appendices in late March. As explained in previous iterations, the CMMC is a method by which the Pentagon will be able determine if Defense Industrial Base (DIB) companies can meet cybersecurity safeguarding and security requirements that govern the handling of two groups of information shared with those entities: Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The CMMC Accreditation Body held a webinar on April 6 "featuring introductory comments from Katie Arrington, Chief Information Security Officer for Acquisition at the Department of Defense and a panel of Accreditation Body board committee chairs" with more webinars to come.

In late January, at the press rollout of CMMC version 1.0, Under Secretary of Defense for Acquisition and Sustainment Ellen Lord explained future CMMC-related actions:

- Now that we have released the public model today, we are now focusing on the remaining CMMC timeline, selecting third-party vendors, rulemaking and completing a memorandum of understanding with the newly-established CMMC accreditation body. Specifically, we are looking at late spring/early summer timeframe to complete a new defense acquisition regulation, a new Defense Federal Acquisition Regulation, or DFAR.
- Next in the timeline will be the CMMC requirement in selected RFIs [request for information] in the June 2020 timeframe, followed by corresponding RFPs [request for proposals] in September 2020 time frame, where CMMC standards will be required at the time of contract award.

The DOD's new certification model to drive better cyber and data security practices among contractors was refreshed as the Pentagon is still planning on a rulemaking to make the CMMC part of contracts and procurement with RFPs and RFIs containing these requirements as soon as this summer.

- We continue to work to select third-party certification vendors. There are multiple companies that are interested right now, but we have not officially designated who is qualified. We will keep you updated.
- Earlier this month, the CMMC accreditation body was created. It is made up of unbiased parties that will oversee the training, quality and administration of the CMMC third-party assessment organizations, and of course, we have a new acronym for you.

Although given the impact of COVID-19, it is entirely possible this timeline slips.

In the revised CMMC, the DOD explained "[a]s part of multiple lines of effort focused on the security and resiliency of the DIB sector, the DOD is working with industry to enhance the protection of the following types of unclassified information within the supply chain:

- Federal Contract Information (FCI): FCI is information provided by or generated for the Government under contract not intended for public release.
- Controlled Unclassified Information (CUI): CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

The DOD stated the CMMC model "measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats...[and] consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community."

The DOD added "[t]he model encompasses the basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for CUI specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204- 7012." DOD stated thhat "[t]he CMMC framework adds a certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level...[and] is designed to provide increased assurance to the DOD that a DIB contractor can adequately protect CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain." Finally, the DOD said "[w]hen implementing CMMC, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for particular segment(s) or enclave(s), depending upon where the information to be protected is handled and stored."

EC Calls For EU-Wide Approach on Big Data and COVID-19

The first priority for the Toolbox should be a pan-European approach for COVID-19 mobile applications, to be developed together by Member States and the Commission, by 15 April 2020…
The second priority for the Toolbox should be a common approach for the use of anonymised and aggregated mobility data….

The European Commission (EC) met in Brussels this week and issued a recommendation outlining what it hopes will be a unified approach throughout the European Union (EU) on how smartphones and data are used to fight the spread of COVID-19. The EC laid out an ambitious timeline and explained "[t]he first priority for the Toolbox should be a pan-European approach for COVID-19 mobile applications, to be developed together by Member States and the Commission, by 15 April 2020." The EC added that "[t]he European Data Protection Board (EDPB) and the European Data Protection supervisor (EDPS) will be associated to the process." The EC stated "[t]he second priority for the Toolbox should be a common approach for the use of anonymised and aggregated mobility data necessary" for a range of purposes to model, predict, and track the virus throughout the EU. On this second priority, the EC is calling for measures to ensure anonymization, safeguarding, and permanent deletion after these data are no longer needed.

It bears note that the EC is working within the structure provided by the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications (the ePrivacy Directive), and other statutes and regulations. In its press release, the EC asserted "[t]o support Member States, the Commission will provide guidance including on data protection and privacy implications…[and] is in close contact with the EDPB for an overview of the processing of personal data at national level in the context of the coronavirus crisis." The EC also remarked on its 23 March call with the heads of EU telecommunications companies and GSMA, their association, that "also covered the need to collect anonymised mobile metadata to help analysing the patterns of diffusion of the coronavirus, in a way that is fully compliant with the GDPR and ePrivacy legislation."

The EC declared

> The public health crisis caused by the current COVID-19 pandemic (hereinafter, 'COVID-19 crisis') is compelling the Union and the Member States to face an unprecedented challenge to its health care systems, way of life, economic stability and values. No single Member State can succeed alone in combating the COVID-19 crisis. An exceptional crisis of such magnitude requires determined action of all Member States and EU institutions and bodies working together in a genuine spirit of solidarity.

The EC continued

> Since the beginning of the COVID-19 crisis, a variety of mobile applications have been developed, some of them by public authorities, and there have been calls from Member States and the private sector for coordination at Union level, including to address cybersecurity, security and privacy concerns. These applications tend to serve three general functions:

(i) informing and advising citizens and facilitating the organisation of medical follow-up of persons with symptoms, often combined with a self-diagnosis questionnaire;
(ii) warning people who have been in proximity to an infected person in order to interrupt infection chains and preventing resurgence of infections in the reopening phase; and
(iii) monitoring and enforcement of quarantine of infected persons, possibly combined with features assessing their health condition during the quarantine period.

Certain applications are available to the general public, while others only to closed user groups directed at tracing contacts in the workplace. The effectiveness of these applications has generally not been evaluated. Information and symptom-checker apps may be useful to raise awareness of citizens. However, expert opinion suggests that applications aiming to inform and warn users seem to be the most promising to prevent the propagation of the virus, taking into account also their more limited impact on privacy, and several Member States are currently exploring their use.

The EC found

A common Union approach to the COVID-19 crisis has also become necessary since measures taken in certain countries, such as the geolocation-based tracking of individuals, the use of technology to rate an individual's level of health risk and the centralisation of sensitive data, raise questions from the viewpoint of several fundamental rights and freedoms guaranteed in the EU legal order, including the right to privacy and the right to the protection of personal data. In any event, pursuant to the Charter of Fundamental Rights of the Union, restrictions on the exercise of the fundamental rights and freedoms laid down therein must be justified and proportionate. Any such restrictions should, in particular, be temporary, in that they remain strictly limited to what is necessary to combat the crisis and do not continue to exist, without an adequate justification, after the crisis has passed.

The EC explained the purpose of the recommendation:

(1) This recommendation sets up a process for developing a common approach, referred to as a Toolbox, to use digital means to address the crisis. The Toolbox will consist of practical measures for making effective use of technologies and data, with a focus on two areas in particular:
(1) A pan-European approach for the use of mobile applications, coordinated at Union level, for empowering citizens to take effective and more targeted social distancing measures, and for warning, preventing and contact tracing to help limit the propagation of the COVID-19 disease. This will involve a methodology monitoring and sharing assessments of effectiveness of these applications, their interoperability and cross-border implications, and their respect for security, privacy and data protection; and
(2) A common scheme for using anonymized and aggregated data on mobility of populations in order (i) to model and predict the evolution of the disease, (ii) to monitor the effectiveness of decision-making by Member States' authorities on measures such as social distancing and confinement, and (iii) to inform a coordinated strategy for exiting from the COVID-19 crisis.
(2) Member States should take these actions as a matter of urgency and in close coordination with other Member States, the Commission and other relevant stakeholders,

> and without prejudice to the competences of the Member States in the domain of public health. They should ensure that all actions are taken in accordance with Union law, in particular law on medical devices and the right to privacy and the protection of personal data along with other rights and freedoms enshrined in the Charter of Fundamental Rights of the Union. The Toolbox will be complemented by Commission guidance, including guidance on the data protection and privacy implications of the use of mobile warning and prevention applications.

The EC added "[t]he EDPB and the EDPS should also be closely involved to ensure the Toolbox integrates data protection and privacy-by-design principles."

The EC stated that "[t]he first priority for the Toolbox should be a pan-European approach for COVID-19 mobile applications, to be developed together by Member States and the Commission, by 15 April 2020" that "should consist of:

> (1) specifications to ensure the effectiveness of mobile information, warning and tracing applications for combating COVID-19 from the medical and technical point of view;
> (2) measures to prevent proliferation of applications that are not compatible with Union law, to support requirements for accessibility for persons with disabilities, and for interoperability and promotion of common solutions, not excluding a potential pan-European application;
> (3) governance mechanisms to be applied by public health authorities and cooperation with the ECDC;
> (4) the identification of good practices and mechanisms for exchange of information on the functioning of the applications; and
> (5) sharing data with relevant epidemiological public bodies and public health research institutions, including aggregated data to ECDC.

Regarding the second principle for the Toolbox, the EC stated it "should be guided by privacy and data protection principles" including:

> (1) safeguards ensuring respect for fundamental rights and prevention of stigmatization, in particular applicable rules governing protection of personal data and confidentiality of communications;
> (2) preference for the least intrusive yet effective measures, including the use of proximity data and the avoidance of processing data on location or movements of individuals, and the use of anonymised and aggregated data where possible;
> (3) technical requirements concerning appropriate technologies (e.g. Bluetooth Low Energy) to establish device proximity, encryption, data security, storage of data on the mobile device, possible access by health authorities and data storage;
> (4) effective cybersecurity requirements to protect the availability, authenticity integrity, and confidentiality of data;
> (5) the expiration of measures taken and the deletion of personal data obtained through these measures when the pandemic is declared to be under control, at the latest;
> (6) uploading of proximity data in case of a confirmed infection and appropriate methods of warning persons who have been in close contact with the infected person, who shall remain anonymous; and
> (7) transparency requirements on the privacy settings to ensure trust into the applications.

The EC added it "will publish guidance further specifying privacy and data protection principles in the light of practical considerations arising from the development and implementation of the Toolbox."

EU's Data Supervisor Calls For Limits On Using Data In Fighting COVID-19

Ahead of the European Commissions' (EC) recommendation on a technological and data-driven European Union-wide approach to fighting COVID-19, the European Data Protection Supervisor (EDPS) Wojciech Wiewiórowski outlined his perspective on these issues in a speech, likely to inform and influence the EC's thinking and the public debate. As more governments around the world have turned directly to telecommunications providers for location data or have bought these data from private sector entities, Wiewiórowski is seeking to ensure that the the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications (aka the ePrivacy Directive) are respected.

"Data protection law calls at the same time for the respect to the essence of the right to data protection and provides suitable and specific measures to safeguard the fundamental rights and the interests of the persons. Even when we recognize that an unusual way of processing would interfere with the right to privacy and data protection, it may still be necessary in the extraordinary circumstances we are all living over the last few weeks."
European Data Protection Supervisor
Wojciech Wiewiórowski

Wiewiórowski contended

> digital solidarity, which should make data working for all people in Europe and especially for those the most vulnerable. Digital solidarity would refuse to replicate the now tarnished and discredited business models of constant surveillance and targeting that have so damaged trust in the digital society but will allow data protection serve mankind during this extraordinary exam in our knowledge, skills and our human values.

Wiewiórowski claimed "[t]he digital revolution has given us powerful tools to process information about the world we live in, about us –human beings –and about our behavior" He remarked that "[o]ur "mantra" is that big data means big responsibility…[and] [w]e have to know what we are doing, and to know that we are responsible for the results of our activity." Wiewiórowski stressed "[r]esponsibility also means however that we should not hesitate to act when it is necessary…[and] [t]here is also responsibility for not using the tools we have in our hands to fight the pandemic."

Wiewiórowski stated

> This is why the EDPS is co-operating with the other European Institutions to give a European response mitigating as much as possible any risks for the fundamental rights of individuals. We appreciate the attention these fundamental rights –including right to data protection – gain among European Union politicians and among European administration, scientists and representatives of market. They all work now hand in hand to find solutions on all-European

> and on national level bearing in mind both European Charter of Fundamental Rights, the GDPR and the European Human Rights Convention.

Wiewiórowski asserted that "[l]egality of processing the personal data –even so called sensitive data like data about health –can be achieved when processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued." He added "[t]he GDPR also permits processing of sensitive data when it is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health."

Wiewiórowski stated

> You can sometimes hear today the call to suspend data protection law or revise it in light of the current crisis. Let me stress again this law is neither an obstacle for being active nor an excuse that we are not efficient as this law was written with consultation of experienced specialists in extraordinary use of new technologies serving the mankind. Data protection law calls at the same time for the respect to the essence of the right to data protection and provides suitable and specific measures to safeguard the fundamental rights and the interests of the persons. Even when we recognize that an unusual way of processing would interfere with the right to privacy and data protection, it may still be necessary in the extraordinary circumstances we are all living over the last few weeks.

Wiewiórowski concluded that "[t]herefore, we are going to work with the EC to make sure that any measures taken at European or national level are:

- Temporary–they are not here to stay after the crisis.
- Their purposes are limited–we know what we are doing.
- Access to the data is limited –we know who is doing what.
- We know what we will do both with results of our operations and with raw data used in the process –we know the way back to normality."

EDPB Fast Tracks Privacy and Processing Guidance For COVID-19

During a plenary session this week, the European Data Protection Board (EDPB or Board) announced in a press release "concrete mandates to its expert subgroups to develop guidance on several aspects of data processing in the fight against COVID-19:

> 1. geolocation and other tracing tools in the context of the COVID-19 outbreak – a mandate was given to the technology expert subgroup (TECH ESG) for leading this work;
> 2. processing of health data for research purposes in the context of the COVID-19 outbreak – a mandate was given to the compliance, e-government and health expert subgroup (CEH ESG) for leading this work."

"The EDPB will move swiftly to issue guidance on these topics within the shortest possible notice to help make sure that technology is used in a responsible way to support and hopefully win the battle against the corona pandemic. I strongly believe data protection and public health go hand in hand." EDPB Chair Andrea Jelinek

Moreover, the EDPB is deciding to set aside its planned "guidance work on teleworking tools and practices in the context of the COVID-19 outbreak" to work on these two mandates. The Board consists of the European Union's (EU) data protection authorities (DPA) and guidance from this entity will likely inform how these DPAs will view the technology deployed to counter COVID-19, especially location data and related means of tracking people and how these data are processed, stored, and disposed of. The EDPB will be applying the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications (the ePrivacy Directive) in construing legal and illegal means, which will further flesh out appropriate uses in other data processing and privacy contexts.

In the TECH ESG's mandate, the EDPB explained "[f]ollowing the remote plenary meeting on 3 April 2020, the EDPB decided to provide guidance on data protection issues arising in the context of the COVID-19 crisis." Consequently, the Board stated "[g]uidance on the issues relating to data protection and the use of tracking and geolocation tools in the context of the COVID-19 outbreak was identified as a priority." The EDPB explained "the TECH ESG is asked to focus in particular on the following issues:

- the use of aggregated / anonymised location data (e.g. provided by telecom or information society service providers) and the effectiveness of aggregation and anonymization techniques;
- the application of the principles of lawfulness, necessity, proportionality, including accuracy, and data minimisation to the different means available to gather location data or trace interactions between data subjects;
- general legal analysis of the use of apps and collection of personal data by apps to help contain the spread of the virus;
- the required safeguards to ensure the respect of data protection principles, including with regard to data retention, in the context of using geo-location or other tracing tools.
- the identification of recommendations or functional requirements for contact tracing applications;
- the necessity to subject the measures taken to a pre-defined timeframe limited to what is strictly necessary to tackle the emergency situation;"

In the mandate to the CEH ESG, the Board explained that this work flows from the same consideration that informed the TECH ESG's. Accordingly, the CEH ESG "is asked to focus in particular on the following issues:

- Processing of health data for the purpose of advancing scientific and medical research connected to the COVID-19 crisis;
- legal basis, principle of proportionality, information and exercise of the rights of data subjects (right to object, right to erasure, etc.), retention period, etc.;
- Re-use of medical research data connected to the COVID-19 crisis and data sharing;•Information and exercise of the rights of data subjects in an emergency situation."

Warner Asks OMB For Uniform Guidance On Contractors

> **"Section 3610 of the CARES Act allows government agencies to continue to pay contractors if they cannot perform their work because of coronavirus-related restrictions, such as the closure of federal or contractor facilities and/or the inability to telework...[and] [s]uch restrictions disproportionately affect contractors who perform classified work that cannot be undertaken outside of a secure facility."** Senator Mark Warner (D-VA)

Senator Mark Warner (D-VA) has written the acting Director of the Office of Management and Budget (OMB) urging him to provide clarity and direction in how federal agencies implement a provision regarding contractors' pay in the last stimulus package, the "Coronavirus Aid, Relief, and Economic Security Act" (CARES Act) (P.L. 116-136). Based on his press release and letter, it seems clear he's talking about contractors with a security clearance who would normally be required to report to a government facility but cannot now because of COVID-19. Warner is pushing for uniform guidance out of OMB to ensure that such contractors who are not allowed to work at these government facilities are still paid. He claimed that different agencies are taking different approaches. To cite one example, on the Director of National Intelligence's guidance page on COVID-19, the DNI stated "[i]f you are a contractor and are unsure if you should report to work, please contact your program manager or company for additional guidance," which is the extent of public guidance from the DNI. However, the DOD has issued more extensive guidance on telework, some of which pertains to contractors with security clearances.

In his press release, Warner asserted "Section 3610 of the CARES Act allows government agencies to continue to pay contractors if they cannot perform their work because of coronavirus-related restrictions, such as the closure of federal or contractor facilities and/or the inability to telework...[and] [s]uch restrictions disproportionately affect contractors who perform classified work that cannot be undertaken outside of a secure facility."

In his letter, Warner called on OMB to "promptly issue a directive so that government agencies consistently implement Sec. 3610...which provides relief to the contractor community supporting many critical national security missions." He cautioned that "[w]ithout such overarching directive, I fear that agencies and their contracting officers will take disparate approaches, leading to uncertainty and instability in the contractor industrial base, if not a permanent loss of capability." Warner claimed that "[a]gencies are already issuing memoranda on this topic that potentially diverge from one another...[and] I want to avoid draconian cutbacks that may create significant counterintelligence risks."

Warner asked OMB to "issue a directive that:

- Fully endorses and supports contractors teleworking or otherwise working remotely, and payment therewith, consistent with mission requirements, law, and Office of Personnel Management memorandum M-18-20, "Managing Federal Contract Performance Issues associated with the Novel Coronavirus (COVID-19)";
- Applies equally to contractor work conducted at government or contractor facilities or sites, whether they support unclassified or classified work;

- Provides a fair cost reimbursement methodology that allows for reasonable direct and indirect costs and in-progress payments for work normally paid on a lump-sum basis;
- Provides standard contract modification language, preferably made available within 15 days of issuance of OMB guidance, to maintain ready state (on-call) contractor capability, reflects dependencies on subcontractors and suppliers whose performance may be impaired by COVID- 19, and adjust contract performance issues, including reductions in scope or schedule changes due to COVID-19;
- Allows expedited consideration of extensions in periods of performance and adjustments in contract ceiling values to minimize unnecessary disruption in contract execution for the duration of the emergency; and
- Applies to contractor work done for all government agencies to the greatest extent practicable to promote consistency for existing and new work."

OCR Announces HIPAA Enforcement Discretion

As part of the federal government's attempt to get a handle on COVID-19, the Department of Health and Human Services' (HHS) Office of Civil Rights (OCR) announced its intention to allow further violations of the regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Put simply, OCR will allow business associates to violate the Privacy Rule if they do so in good faith in sharing Protected Health Information (PHI) with the CDC, CMS, or state agencies to assist in their public health oversight or public health activities related to combatting COVID-19.

As a matter of enforcement discretion, effective immediately, the HHS Office for Civil Rights (OCR) will exercise its enforcement discretion and will not impose potential penalties for violations of certain provisions of the HIPAA Privacy Rule against covered health care providers or their business associates for uses and disclosures of protected health information by business associates for public health and health oversight activities during the COVID-19 nationwide public health emergency.

OCR explained:

> This notification is to inform the public that the Department of Health and Human Services (HHS) is exercising its discretion in how it applies the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Current regulations allow a HIPAA business associate to use and disclose protected health information for public health and health oversight purposes only if expressly permitted by its business associate agreement with a HIPAA covered entity. As a matter of enforcement discretion, effective immediately, the HHS Office for Civil Rights (OCR) will exercise its enforcement discretion and will not impose potential penalties for violations of certain provisions of the HIPAA Privacy Rule against covered health care providers or their business associates for uses and disclosures of protected health information by business associates for public health and health oversight activities during the COVID-19 nationwide public health emergency.

OCR explained that "[t]he HIPAA Privacy Rule permits a business associate of a HIPAA covered entity to use and disclose PHI to conduct certain activities or functions on behalf of the covered

entity, or provide certain services to or for the covered entity, but only pursuant to the explicit terms of a business associate contract or other written agreement or arrangement under 45 CFR 164.502(e)(2) (collectively, "business associate agreement" or BAA), or as required by law."

However, OCR spelled out the limits of discretion through this notice:

> To facilitate uses and disclosures for public health and health oversight activities during this nationwide public health emergency, effective immediately, OCR will exercise its enforcement discretion and will not impose penalties against a business associate or covered entity under the Privacy Rule provisions 45 CFR 164.502(a)(3), 45 CFR 164.502(e)(2), 45 CFR 164.504(e)(1) and (5) if, and only if:
>
> - the business associate makes a good faith use or disclosure of the covered entity's PHI for public health activities consistent with 45 CFR 164.512(b), or health oversight activities consistent with 45 CFR 164.512(d); and
> - the business associate informs the covered entity within ten (10) calendar days after the use or disclosure occurs (or commences, with respect to uses or disclosures that will repeat over time).

Examples of such good faith uses or disclosures covered by this Notification include uses and disclosures for or to:

- the Centers for Disease Control and Prevention (CDC), or a similar public health authority at the state level, for the purpose of preventing or controlling the spread of COVID-19, consistent with 45 CFR 164.512(b).
- the Centers for Medicare and Medicaid Services (CMS), or a similar health oversight agency at the state level, for the purpose of overseeing and providing assistance for the health care system as it relates to the COVID-19 response, consistent with 45 CFR 164.512(d).

Executive Order Formalizes Review of Foreign Investment in Telecommunications

President Donald Trump has issued an executive order creating an inter-agency review body to determine whether foreign investment in U.S. telecommunications companies presents national security issues. However, the executive order merely formalizes and change the longstanding "Team Telecom" process through which proposed foreign investment in the U.S. telecommunications industry have been evaluated. Like the previous body, the new body will consist of representatives from the Departments of Defense, Homeland Security, and Justice and other agencies in an advisory role. Notably, a time limit will be set on how long these reviews should take. Moreover, a number of the changes will align this review process with the reforms enacted in 2018 to the Committee for Foreign Investment in the United States (CFIUS) process, and like the recent reforms to CFIUS, many of these reforms are aimed at countering Chinese companies' growing investment in or purchase of U.S. companies in key industries.

> **As we demonstrated last year in rejecting the China Mobile application, this FCC will not hesitate to act to protect our networks from foreign threats…[but] [a]t the same time, we welcome beneficial investment in our networks and believe that this Executive Order will allow us to process such applications more quickly."**
> FCC Chair Ajit Pai

The Executive Order (EO) "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector" creates the new "Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector" (Committee) chaired by the Attorney General. The EO explained "the primary objective of which shall be to assist the Federal Communications Commission (FCC) in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector." Moreover, the "The function of the Committee shall be:

> (i) to review applications and licenses for risks to national security and law enforcement interests posed by such applications or licenses; and
> (ii) to respond to any risks presented by applications or licenses by recommending to the FCC, as appropriate and consistent with the provisions of this order, that it dismiss an application, deny an application, condition the grant of an application upon compliance with mitigation measures, modify a license with a condition of compliance with mitigation measures, or revoke a license."

The Committee "shall review and assess applications to determine whether granting a license or the transfer of a license poses a risk to national security or law enforcement interests of the United States" and must render its assessment within 120 days. If a secondary assessment is required "is warranted because risk to national security or law enforcement interests cannot be mitigated by standard mitigation measures," then an additional 90 day review period may commence.

In a statement, Federal Communications Commission Chairman Ajit Pai said, "I applaud the President for formalizing Team Telecom review and establishing a process that will allow the Executive Branch to provide its expert input to the FCC in a timely manner." He claimed that "[n]ow that this Executive Order has been issued, the FCC will move forward to conclude our own pending rulemaking on reform of the foreign ownership review process." Pai stated that "[a]s we demonstrated last year in rejecting the China Mobile application, this FCC will not hesitate to act to protect our networks from foreign threats…[but] [a]t the same time, we welcome beneficial investment in our networks and believe that this Executive Order will allow us to process such applications more quickly."

The pending rulemaking to which Pai referred was started under his predecessor former chair Tom Wheeler and would change the FCC's review of foreign applications in these ways:

> In this Notice of Proposed Rulemaking, we propose changes to our rules and procedures related to certain applications and petitions for declaratory ruling involving foreign ownership(together, "applications"). As discussed below, the Commission refers certain applications to the relevant Executive Branch agencies for their input on any national security, law enforcement, foreign policy, and trade policy concerns that may arise from the foreign ownership interests held in the applicants and petitioners (together, "applicants"). As part of our effort to reform the Commission's processes, we seek to improve the timeliness and transparency of this referral process. More specifically, our goals here are to identify ways in which both the Commission and the agencies might streamline and facilitate the process for obtaining information necessary for Executive Branch review and identify expected time frames, while ensuring that we continue to take Executive Branch concerns into consideration as part of our public interest review.

CISA Guides Agencies On Telework Best Practices and Security

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued guidance to federal agencies to help them establish and maintain telework for their employees and contractors that comports with a recently revamped program to ensure that federal civilian agencies are limiting their cyber risk and exposure. The ad hoc guidance comes at a time when many federal employees and contractors are working from work, thus raising all sorts of security issues given the sensitivity of information some receive and handle.

In the TIC 3.0 Interim Telework Guidance, CISA stated "this document provides security capabilities for remote federal employees securely connecting to private agency networks and cloud environments." The agency cautioned that "[t]he guidance is short-term for Calendar Year (CY) 2020 and is expected to be incorporated into a Remote User Use Case later."

Teleworkers require access to resources on the agency campus, agency-sanctioned cloud services, and on the public web. Each of these security patterns presents unique risks and corresponding security capabilities for appropriate use. This document will focus on TIC 3.0 adaptations for communication between teleworkers and agency-sanctioned cloud services. Teleworker communications with agency campus hosted resources and with web entities should continue to follow established agency protections.

CISA stated that "[a]s federal civilian agencies respond to the COVID-19 situation, the number of federal agency employees working remotely has increased dramatically…[and] [i]n order to support agencies as they respond to this surge in teleworking, CISA is issuing this interim TIC guidance to help agencies leverage existing resources to secure their networks." CISA said that "[t]he purpose of this document is to help federal civilian agencies address the telework surge concerns by:

- Providing awareness that the security patterns outlined under Agency Teleworker Options 1 and 2 (below) align to TIC architecture capabilities as presented in the draft TIC 3.0 guidance (December 2019).
    - Agencies should ensure that appropriate data sharing is maintained with Agency Security Operations Centers.
    - Agencies should be prepared to discuss the availability of log and telemetry features in order to determine what relevant information will need to be provided to CISA for cybersecurity analytical purposes.
- Informing agencies that the interim guidance provided under Agency Teleworker Option 3 provides additional temporary relief with additional security patterns.
- Suggesting security capabilities for agencies to consider when creating or expanding their teleworking platforms.
- Allowing vendors to map the cybersecurity capabilities provided by their services to the TIC security capabilities that support secure teleworking."

CISA stressed

- This document is only intended to address the current teleworking surge. It is not intended to be part of the TIC 3.0 document set or support a TIC 3.0 use case; it will be deprecated at the end of 2020. The guidance is not intended to be comprehensive and should not be interpreted as a use case nor reference architecture. Agencies can refer to the TIC 3.0 document set for more details on the TIC program and objectives, additional TIC 3.0 guidance, and clarification of TIC terminology used throughout this document. This interim guidance will be integrated into the TIC 3.0 Remote User Use Case at a later date.
- The COVID-19 situation presents unique cybersecurity threats, and agencies must consider these unique threats when securing their platforms. This document identifies a subset of the security capabilities detailed in the TIC 3.0 Security Capabilities Handbook that are applicable to the current telework surge and can be used to prevent, mitigate, and detect some of these emerging threats. This document also introduces new TIC security capabilities that are unique to telework. The full set of TIC security capabilities can be found in the TIC 3.0 TIC Security Capabilities Handbook.
- This document is only intended to address scenarios in which agency users connect remotely to agency-sanctioned cloud environments. Any traffic to the public internet (i.e., public web traffic) must still be routed through EINSTEIN sensors, the operational capabilities of the National Cybersecurity Protection System (NCPS) program3. When in doubt, agency traffic should be routed through EINSTEIN sensors.
- Vendors will be responsible for mapping their service offerings to the suggested TIC objectives and security capabilities. Agencies and vendors should work together to identify appropriate implementation approaches that focus on improving employment of capabilities and services in alignment with agency risk tolerances.
- Agencies, in consultation with appropriate vendors, will coordinate the expansion of cloud and collaboration services that deviate from existing reference architectures to ensure that CISA programs are notified. Agencies should be prepared to discuss the availability of log and telemetry features in order to determine what relevant information will need to be provided to CISA for cybersecurity analytical purposes.

In September 2019, the Office of Management and Budget (OMB) released its long-awaited revision of the TIC initiative that is of a piece with the Trump Administration's push to modernize the federal government's information technology (IT), notably by moving as much of operations as possible and feasible to the cloud. The Department of Homeland Security (DHS) will define what constitutes "TIC Use Cases" that will define alternative standards and processes that agencies may ultimately use instead of TIC. To this end, "DHS, in coordination with OMB and the Federal Chief Information Security Officer (CISO) Council shall establish and publicly release a detailed process document."

OMB explained

> The purpose of the TIC initiative is to enhance network security across the Federal Government. Initially, this was done through the consolidation of external connections and the deployment of common tools at these access points. While this prior work has been invaluable in securing Federal networks and information, the program must adapt to modem architectures and frameworks for government IT resource utilization. Accordingly, this memorandum provides an enhanced approach for implementing the TIC initiative that provides agencies with increased flexibility to use modern security capabilities. This memorandum also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats.

Further Reading

- "Taiwan joins Canada in banning Zoom for government video conferencing" – *CBC* and "Video service Zoom taking security seriously: U.S. government memo" – *Reuters*. The island nation joined Canada in banning the use of popular web conferencing app, Zoom, even though the company is allegedly addressing security concerns turned up over the last few weeks. Taiwan's Cabinet cited "security concerns" without identifying those concerns in its statement recommending the use of other apps. However, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Federal Risk and Authorization Management Program reportedly issued a memorandum finding the government version of Zoom safe to use, which is different from its free or business versions. Citizen Lab has issued a report calling into question Zoom's security, among other things, however.
- "We Saw NSO's Covid-19 Software in Action, and Privacy Experts Are Worried" – *Vice's Motherboard*. Israel's NSO Group and Italy's Cy4Gate have pitched systems to their respective governments and possibly others that would use people's phones to track them in the name of preventing and tracing COVID-19. NSO Group's system allegedly uses the contacts in one's phone to suss out who a person has contacted or is liable to contact. Cy4Gate would rely more on location data to much the same aims. Questions have been raised from the perspective of civil liberties and privacy and effectiveness. Thus far, as far as is known, it has just been government agencies using location data although there is possibly help from private sector companies.
- "The Far-Right Helped Create The World's Most Powerful Facial Recognition Technology" – *HuffPost*. A long read on Clearview AI and its ties to white supremacists, Neo-Nazis, and Peter Thiel, who has invested in Clearview and owns a large stake in Palantir which contracts with numerous federal agencies to provide data analytics. This epic examination of all the interconnections is worth the time.
- "The Humble Phone Call Has Made a Comeback" – *The New York Times*. In a somewhat surprising development, Verizon is saying that boring, vanilla wireless calls have risen by 50% and AT&T says the same on their networks has increased 35%. Everyone quoted in the article claims this is because sheltering-in-place Americans are looking for connection in the form of voice. The article hints that over the top call services like WhatsApp are also experiencing surges, and, of course, the now ubiquitous Zoom has experienced phenomenal growth. However, something the article touches on but does not develop is the possibility that internet capacity issues may be limiting video calls and so phone calls are a more appealing option.
- "As School Moves Online, Many Students Stay Logged Out" – *The New York Times*. As should not be a surprise for anyone with even just a rudimentary grasp of the Digital Divide, more affluent children are participating in distance learning programs at a much higher rate due to a variety of reasons, including a household's inability to afford broadband service, an area's spotty or non-existent coverage, or new duties foist on children by parents who still need to work outside the home. It would seem absent dramatic, even miraculous, changes in federal and state programs and funding, the gap between the digital haves and haves not will only grow with the differences in the education of American children growing as well.
- "Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance" – *The Washington Post*. Another feature of digital life that has accelerated during the COVID-19 pandemic: online proctors for tests. However, allowing these proctors to access laptop cameras, microphones, and screens present all sorts of privacy issues, in addition to the other software and apps universities and high schools are using to surveil

their students. More dramatically, some companies use facial recognition technology, eye-tracking software, and even predictive software to determine whether a student is cheating. Moreover, these companies get access to all sorts of sensitive student data in the name of ensuring the person taking the test is actually who she claims to be. And, many students have to pay fees for the service they are being forced to use.

- "WhatsApp to impose new limit on forwarding to fight fake news" – *The Guardian*. The popular messaging app is trying to slow the spread of COVID-19 misinformation and lies by setting new limits on the forwarding of certain messages. Now, if a message has been forwarded five or more times, a user will only be able to send it on to one person or chat at a time. In 2018, WhatsApp instituted a five person/chat forward limit in India where the mass forwarding of rumors and fake news led to the lynchings of more than 30 people who were allegedly kidnapping children. This limit was extended to the rest of the world in 2019. Presently, there are WhatsApp messages indicating that 5G is the cause of COVID-19 and all manner of pseudo-science and incorrect medical advice being sent via WhatsApp.