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

CARES Act Largely Bypasses Tech Funding and Issues

On March 27, President Donald Trump signed into law the "Coronavirus Aid, Relief, and Economic Security Act" (CARES Act) (P.L. 116-136), the third stimulus package in the last month, that could cost $2.5 trillion, or even more, once all the spending is accounted for. There are provisions in the package loosening restrictions and increasing funding for telehealth and telework as the demand for both have skyrocketed during the COVID-19 crisis.

There is also additional funding to address cybersecurity issues. Most notably, the Election Assistance Commission (EAC) was given an additional $400 million "to prevent, prepare for, and respond to coronavirus, domestically or internationally, for the 2020 Federal election cycle." The EAC was provided with $380 million and $425 million, respectively in FY 2018 and 2019, to help states tighten the security of their election systems in large part because of Russian hacking and interference during the 2016 election. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) was provided with an additional $9.1 million for FY 2020 and 2021 "to prevent, prepare for, and respond to coronavirus, domestically or internationally, which shall be for support of interagency critical infrastructure coordination and related activities."

Congress will likely pass additional COVID-19 relief and stimulus packages, and there are likely more funding and programmatic changes for technology programs coming. For example, House Democrats released the "The Take Responsibility for Workers and Families Act" (H.R.6379) last week when Senate Republicans, Senate Democrats, and the White House were negotiating the final version of the CARES Act. This $2.5 trillion package embodies many Democratic priorities, including technology policy. For example, the bill would provide CISA with $14.4 million to combat the effects of COVID-19, but that figure is likely the House Democrat's preferred funding level as compared to the $9.1. million that was enacted as part of the CARES Act. And yet, the $4 billion House Democrats wanted for the EAC could augur significantly more funding for the agency to parcel out to states so they can improve and better secure their election systems.

However, the bill would provide $3 billion for the Technology Modernization Fund (TMF), a program that set up a revolving fund in the General Services Administration (GSA) to lend funds to agencies to refresh and replace dated information technology, especially legacy systems. In FY 2020, the Trump Administration asked for $150 million for the program but received only $25 million.

Broadband and 5G could both see additional funding. House Democrats allocated $25 million in extra funding for the Department of Agriculture's Rural Utilities Service (RUS) for "Distance Learning, Telemedicine, and Broadband Program." The first draft of the bill included $2 billion for a new Emergency Connectivity Fund to be established and administered by the Federal Communications Commission (FCC), and the agency would also receive $1 billion for an "Emergency Broadband Connectivity Fund." And, there are additional provisions as detailed in a section-by-section summary prepared by the Democratic staff of the House Energy and Commerce Committee:

- Section 102. Anti-Price Gouging During COVID-19 Emergency. This section provides the Federal Trade Commission and State attorneys general the authority to seek civil penalties from individuals and companies engaging in price gouging of goods and services during the COVID- 19 public health emergency.
- Section 201. Broadband Hotspots and Connected Devices for Schools and Libraries During COVID-19 Emergency. This section authorizes increased funding and provides flexibility to the Federal Communication Commission's (FCC) E-Rate program to enable schools and libraries, including tribal schools and libraries, to offer broadband hotspots and connected devices to facilitate distance learning and connectivity during the COVID-19 public health emergency.
- Section 301. Expansion of Low-Income Broadband Subsidies During COVID-19 Emergency. This section authorizes increased funding and provides flexibility for the FCC's Lifeline program to expand access to broadband for low-income Americans during the COVID- 19 public health emergency.
- Section 401. Telecommunications Consumer Protections During COVID-19 Emergency.
- This section makes certain practices, including the stopping of telephone or broadband services, if a consumer is unable to pay for reasons related to the COVID-19 emergency, unlawful during the COVID-19 public health emergency.
- Section 501. Public Safety Use of the T-Band. This section repeals the requirement on the FCC to reallocate and auction the T-Band (470-512 MHz), which allows first responders to continue the use of the band for their public safety communications.

House Democrats could also use existing legislation or proposals. In the technology space, In May 2019, the chair and most Democrats on the House Energy and Commerce Committee introduced the "Leading Infrastructure For Tomorrow's America Act" (H.R.2741), which was mostly about messaging and establishing a program to differentiate House Democrats from the White House and Senate Republicans. In a summary, Committee Democrats pointed to highlights of the package, most of which are technology-related:

Action to Combat the Climate Crisis and Protect Our Environment:

- **Over $33 billion for clean energy**, including $4 billion to upgrade the U.S. electric grid to accommodate more renewable energy and make it more resilient. It also includes $4 billion for the expansion of renewable energy use, including $2.25 billion for the installation of solar panels in low-income and underserved communities. LIFT America also includes $23 billion for energy efficiency efforts – namely retrofitting and weatherizing buildings, including schools and homes, to ensure they produce fewer carbon emissions – and funding the nationwide deployment of more clean energy fuels.
- **$2.7 billion to spur the development of Smart Communities**, including $850 million in technical assistance to help cities and counties integrate clean energy into their redevelopment efforts, and $1.4 billion to support the development of an electric vehicle (EV) charging network.

Expanding Access to Broadband Internet:

- **$40 billion for the deployment of secure and resilient high-speed broadband internet service** to expand access for communities nationwide and bring broadband to 98 percent of the country.
- **$12 billion in grants for the implementation of Next Generation 9-1-1 services** to make 9-1-1 service more accessible, effective, and resilient, and enable Americans to send text messages, images, or videos to 9-1-1 in times of emergency.

- **$5 billion in federal funding for low-interest financing of broadband infrastructure deployment** through a new program that would allow eligible entities to apply for secured loans, lines of credit, or loan guarantees to finance broadband infrastructure build out projects.

Investing in America's Health Infrastructure:

- **$2 billion in funding to reauthorize the Hill-Burton hospital infrastructure program**, including targeted assistance to support cybersecurity in the health system.
- **$1 billion for Indian Health Service** infrastructure projects to reduce health disparities in Indian Country.
- **$100 million to support state labs** on the frontlines of fighting infectious diseases.
- **$100 million to establish a community-based care infrastructure program** and to develop teaching health centers and mental health care centers.
- **$3.5 billion to improve public health infrastructure at the Centers for Disease Control and Prevention (CDC) and at state, local, tribal and territorial health departments.**

A first draft of the bill contained language requiring the Federal Reserve Bank to set up a system of "pass-through digital dollar wallets" so that direct payments from the U.S. government to Americans as a means of stimulating the economy. So, it is possible this new program or similar language gets included in a fourth COVID-19 stimulus bill.

Finally, there may be growing consensus that a surface transportation reauthorization could be passed that would be much larger than normal and most likely front-loaded in order to stimulate the economy. This week, President Donald Trump called for a $2 trillion-dollar package, which was echoed by House Democrats but It is possible that this bill could be the vehicle by which more broadband, 5G, or technology funding is pushed through existing programs or newly created programs.

Revised CISA Essential Workers Guidance

Over the weekend, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) revised its "Memorandum on Identification of Essential Critical Infrastructure Workers During COVID-19 Response" to further stress that states and local governments would ultimately determine which sectors, functions, and workers would be considered critical and by adding three new sectors that the agency thinks could be considered essential.

First, CISA added the adjective "Advisory" to the title of the memorandum to further emphasize that the document is not meant as binding and that the agency is not directing state and local governments on how to categorize workers essential for critical infrastructure. CISA added this language as well:

> This list is intended to help State, local, tribal and territorial officials as they work to protect their communities, while ensuring continuity of functions critical to public health and safety, as well as economic and national security. Decisions informed by this list should also take into consideration additional public health considerations based on the specific COVID-19-related concerns of particular jurisdictions.

CISA also included, in bold letters, the following:

> **This list is advisory in nature. It is not, nor should it be considered, a federal directive or standard. Additionally, this advisory list is not intended to be the exclusive list of critical infrastructure sectors, workers, and functions that should continue during the COVID-19 response across all jurisdictions. Individual jurisdictions should add or subtract essential workforce categories based on their own requirements and discretion.**

In the first memorandum, In the attached cover letter to the memo, CISA Director Christopher Krebs explained

> **...this list is advisory in nature. It is not, nor should it be considered to be, a federal directive or standard in and of itself.**

So, obviously the agency is hitting the point harder that the federal government is not in charge of determining which workers, sectors, and functions are to be considered critical. This would be of a piece with much of the Trump Administration's response to COVID-19 in allowing states to determine, for example, whether to issue stay-at-home orders. And yet, there appears to be the risk that some sectors, functions, or workers may be categorized as essential in one jurisdiction, but not another, which carries risk that a sector CISA and the federal government would normally consider critical is not treated as such at the state level. And this could expose it to increased risk of a cyber-attack, among other dangers.

CISA continued in the cover letter of the new memorandum:

> State, local, tribal, and territorial governments are responsible for implementing and executing response activities, including decisions about access and reentry, in their communities, while the Federal Government is in a supporting role. Officials should use their own judgment in issuing implementation directives and guidance. Similarly, while adhering to relevant public health guidance, critical infrastructure owners and operators are expected to use their own judgement on issues of the prioritization of business processes and workforce allocation to best ensure continuity of the essential goods and services they support. All decisions should appropriately balance public safety, the health and safety of the workforce, and the continued delivery of essential critical infrastructure services and functions. While this advisory list is meant to help public officials and employers identify essential work functions, it allows for the reality that some workers engaged in activity determined to be essential may be unable to perform those functions because of health-related concerns.

CISA expanded the types of workers and considerations for most of the sectors identified in the first memorandum, but added three new sectors: Commercial Facilities, Residential/Shelter Facilities And Services, and Hygiene Products And Services.

U.S. and Other Governments Respond To Privacy and Data Implications of COVID-19

Federal agencies have continued to respond to the changing conditions presented by the increased number of COVID-19. However, while the U.S. government has not weighed in officially on the legality and appropriateness of using people's location data from phones in order to combat the spread of the virus, European authorities have.

Last week, the Federal Trade Commission (FTC) sought to assure businesses and other regulated entities that the agency would look kindly on some activities that might otherwise be anti-competitive if the ultimate goal is to help consumers get by and survive COVID-19. Yet, the agency made clear that it would continue to police unfair and deceptive practices.

FTC Chair Joe Simons issued a statement explaining that "FTC staff in the Bureau of Consumer Protection remain hard at work protecting consumers from deceptive and unfair commercial practices" but "the FTC will remain flexible and reasonable in enforcing compliance requirements that may hinder the provision of important goods and services to consumers." Simons added "[t]o be clear, by being flexible and reasonable, I am not suggesting that we will tolerate companies deceiving consumers, using tactics that violate well-established consumer protections, or taking unfair advantage of these uniquely challenging times…[and] [a]t all times, good faith efforts undertaken to provide needed goods and services to consumers will be taken into account in making enforcement decisions." He stated "[t]he FTC is ready to assist businesses that may seek guidance about compliance obligations on consumer protection issues during this unprecedented time."

On April 3, the FTC and the Federal Communications Commission (FCC) transmitted letters " to three companies providing Voice over Internet Protocol (VoIP) services,warning them that routing and transmitting illegal robocalls, including Coronavirus-related scam calls, is illegal and may lead to federal law enforcement against them" per the agencies' press release.

The FTC and FCC noted "a separate letter to USTelecom – The Broadband Association (USTelecom), a trade association that represents U.S.-based telecommunications-related businesses…thanks USTelecom for identifying and mitigating fraudulent robocalls that are taking advantage of the Coronavirus national health crisis, and notes that the USTelecom Industry Traceback Group has helped identify various entities that appear to be responsible for originating or transmitting Coronavirus-related scam robocalls." The agencies stated:

> The letter further notifies USTelecom that if, after 48 hours of the release of the letter, any of the specified gateway or originating providers continue to route or transmit the specified originators' robocalls on its network, the FCC will: 1) authorize other U.S. providers to block all calls coming from that gateway or originating provider; and 2) authorize other U.S. providers to take any other steps as needed to prevent further transmission of unlawful calls originating from the originator.

Last week, FTC staff sent "letters to nine Voice over Internet Protocol (VoIP) service providers and other companies warning them that "assisting and facilitating" illegal telemarketing or robocalls related to the coronavirus or COVID-19 pandemic is against the law" according to the agency's press release. The FTC argued that "[m]any of these calls prey upon consumers' fear of the virus to perpetrate scams or sow disinformation."

Earlier in March, according to the agencies' press release, the FTC and Food and Drug Administration (FDA) "sent warning letters to seven companies allegedly selling unapproved products that may violate federal law by making deceptive or scientifically unsupported claims about their ability to treat coronavirus (COVID-19) [that]…are the first issued by the agencies alleging unapproved and/or unsupported claims that products can treat or prevent coronavirus: 1) Vital Silver, 2) Quinessence Aromatherapy Ltd., 3) N-ergetics, 4) GuruNanda, LLC, 5) Vivify

Holistic Clinic, 6) Herbal Amy LLC, and 7) The Jim Bakker Show." The agencies alleged "[t]he recipients are companies that advertise products—including teas, essential oils, and colloidal silver—as able to treat or prevent coronavirus…[but] [a]ccording to the FDA, however, there are no approved vaccines, drugs, or investigational products currently available to treat or prevent the virus."

The FTC also joined the Department of Justice (DOJ) in a statement "to make clear to the public that there are many ways firms, including competitors, can engage in procompetitive collaboration that does not violate the antitrust laws."

Internationally, agencies with data protection and privacy responsibilities have also moved to remind public and private sector entities of how latitude they have under national law to use personal data to fight COVID-19. The European Data Protection Supervisor (EDPS) Wojciech Wiewiórowski responded to a request from the European Union's Directorate-General for Communications Networks, Content and Technology "on the monitoring of the spread of the COVID-19 outbreak," presumably through the use of location data and metadata to track EU citizens to monitor health and compliance. One of the EDPS' primary duties is to enforce data protection laws on EU agencies.

Wiewiórowski explained

- Firstly, let me underline that data protection rule currently in force in Europe are flexible enough to allow for various measures taken in the fight against pandemics. I am aware of the discussions taking place in some Member States with telecommunications providers with the objective of using such data to track the spread of the COVID-19 outbreak.
- I share and support your call for an urgent establishment of a coordinated European approach to handle the emergency in the most efficient, effective and compliant way possible.
- There is a clear need to act at the European level now.

Wiewiórowski stated that "[o]n the basis of the information provided in your letter and in absence of a more specific data model, please find below some elements for your consideration:

- Data anonymization
    - It is clear from your letter that you intend to use only anonymous data to map movements of people with the objective of ensuring the stability of the internal market and coordinating crisis response. Effectively anonymised data fall outside of the scope of data protection rules
    - At the same time, effective anonymisation requires more than simply removing obvious identifiers such as phone numbers and IMEI numbers. In your letter, you also mention that data would be aggregated, which can provide an additional safeguard.
    - I understand that the Health Security Committee established by Decision (EU) 1082/2013 you make explicit reference to would be the relevant forum for exchanges with the Member States in this case. The Commission should ensure that the data model would enable it to respond to the needs of the users of these analyses. Moreover, the Commission should clearly define the dataset it wants to obtain and ensure transparency towards the public, to avoid any possible misunderstandings. I would appreciate if you could share with me a copy of the data model, once defined, for information.
- Data security and data access

    - As mentioned above, to the extent the data obtained by the Commission would be anonymous, it falls outside the scope of data protection rules. Nonetheless, information security obligations under Commission Decision 2017/464still apply, as do confidentiality obligations under the Staff Regulations for any Commission staff processing the information. Should the Commission rely on third parties to process the information, these third parties have to apply equivalent security measures and be bound by strict confidentiality obligations and prohibitions on further use as well. I would also like to stress the importance of applying adequate measures to ensure the secure transmission of data from the telecom providers. It would also be preferable to limit access to the data to authorised experts in spatial epidemiology, data protection and data science.
- Data retention
    - I also welcome that the data obtained from mobile operators would be deleted as soon as the current emergency comes to an end. It should be also clear that these special services are deployed because of this specific crisis and are of temporary character. The EDPS often stresses that such developments usually do not contain the possibility to step back when the emergency is gone. I would like to stress that such solution should be still recognised as extraordinary.

Wiewiórowski added that he wanted "to recall the importance of full transparency to the public on the purpose and procedure of the measures to be enacted…[and] I would also encourage you to keep your Data Protection Officer involved throughout the entire process to provide assurance that the data processed had indeed been effectively anonymised." Wiewiórowski stressed that "should the Commission feel compelled at any point in the future to change the envisaged modalities for processing, a new consultation of the EDPS would be necessary…[and] [t]he EDPS is ready not only to consult the plans but also to actively involve its resources in the process of development of products and services that may have significant value to the public."

The Office of the Privacy Commissioner of Canada (OPC) issued guidance "to help organizations subject to federal privacy laws understand their privacy-related obligations during the COVID-19 outbreak" according to the agency's press release. OPC explained that "[d]uring a public health crisis, privacy laws still apply, but they are not a barrier to appropriate information sharing." OPC stated that "[t]he new document provides general guidance on applying the Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, and the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal private-sector privacy law, in the context of the current outbreak." OPC added that "[a]ll organizations must continue to operate with lawful authority and exercise good judgment…[and] [g]overnment institutions will need to apply the principles of necessity and proportionality, whether in applying existing measures or in deciding on new actions to address the current crisis." OPC declare it "will continue to protect the privacy of Canadians, while adopting a flexible and contextual approach in its application of the law."

On April 1, the Office of the Australian Information Commissioner (OAIC) issued a press release announcing "privacy guidance for agencies and private sector employers to help keep workplaces safe and handle personal information appropriately as part of the COVID-19 response. This includes:

- Using and disclosing individuals' personal information, including sensitive health information, on a 'need-to-know' basis

- Only collecting, using or disclosing the minimum amount of personal information reasonably necessary to prevent or manage COVID-19
- Advising staff about how their personal information will be handled in responding to any potential or confirmed COVID-19 cases in the workplace
- Taking reasonable steps to keep personal information secure, including where employees are working remotely.

OAIC asserted it and "state and territory privacy regulators have convened a National COVID-19 Privacy Team to respond to proposals with national implications."

OIG Finds More Flaws in FBI FISA Process

The Department of Justice's (DOJ) Office of the Inspector General (OIG) issued another report critical of how the Federal Bureau of Investigation (FBI) has complied with requirements for submitting applications to Foreign Intelligence Surveillance Courts under the Foreign Intelligence Surveillance Act (FISA). Like the previous report in December 2019 investigating the FISA process that led to surveillance of certain members of the Trump presidential campaign, this report also turned up numerous instances under which the FBI was not meeting the requirements to substantiate claims made in FISA applications. This report comes at a time when four FISA authorities have lapsed as the House and Senate could not agree on a final bill, and the House has declined to pass the Senate's extension passed before COVID-19 more or less took over the legislative agenda.

The OIG explained

> As a result of these findings (i.e. the investigation in FBI surveillance of some Trump campaign operatives), in December 2019, my office initiated an audit to examine more broadly the FBI's execution of, and compliance with, its Woods Procedures relating to U.S. Persons covering the period from October 2014 to September 2019. As an initial step in our audit, over the past 2 months, we visited 8 FBI field offices of varying sizes and reviewed a judgmentally selected sample of 29 applications relating to U.S. Persons and involving both counterintelligence and counterterrorism investigations. This sample was selected from a dataset provided by the FBI that contained more than 700 applications relating to U.S. Persons submitted by those 8 field offices over a 5-year period. The proportion of counterintelligence and counterterrorism applications within our sample roughly models the ratio of the case types within that total of FBI FISA applications. Our initial review of these applications has consisted solely of determining whether the contents of the FBI's Woods File supported statements of fact in the associated FISA application; our review did not seek to determine whether support existed elsewhere for the factual assertion in the FISA application (such as in the case file), or if relevant information had been omitted from the application. For all of the FISA applications that we have reviewed to date, the period of court-authorized surveillance had been completed and no such surveillance was active at the time of our review.

The OIG stated that "[a]s a result of our audit work to date and as described below, we do not have confidence that the FBI has executed its Woods Procedures in compliance with FBI policy." The OIG noted that "[s]pecifically, the Woods Procedures mandate compiling supporting documentation for each fact in the FISA application…[and] [a]dherence to the Woods Procedures should result in such documentation as a means toward achievement of the FBI's policy that FISA

applications be 'scrupulously accurate.'" The OIG stated that "[o]ur lack of confidence that the Woods Procedures are working as intended stems primarily from the fact that:

> (1) we could not review original Woods Files for 4 of the 29 selected FISA applications because the FBI has not been able to locate them and, in 3 of these instances, did not know if they ever existed;
> (2) our testing of FISA applications to the associated Woods Files identified apparent errors or inadequately supported facts in all of the 25 applications we reviewed, and interviews to date with available agents or supervisors in field offices generally have confirmed the issues we identified;
> (3) existing FBI and National Security Division (NSD) oversight mechanisms have also identified deficiencies in documentary support and application accuracy that are similar to those that we have observed to date; and
> (4) FBI and NSD officials we interviewed indicated to us that there were no efforts by the FBI to use existing FBI and NSD oversight mechanisms to perform comprehensive, strategic assessments of the efficacy of the Woods Procedures or FISA accuracy, to include identifying the need for enhancements to training and improvements in the process, or increased accountability measures.

However, the OIG cautioned that "[d]uring this initial review, we have not made judgments about whether the errors or concerns we identified were material." The OIG added that "we do not speculate as to whether the potential errors would have influenced the decision to file the application or the FISC's decision to approve the FISA application…[and] our review was limited to assessing the FBI's execution of its Woods Procedures, which are not focused on affirming the completeness of the information in FISA applications."

This is the second report critical of government surveillance programs in the last month. In March, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) released its "Report on the Government's Use of the Call Detail Records Program Under the USA Freedom Act" that noted that in only two instances did the CDR program turn up intelligence that was unique and valuable despite having collected over 434 million CDRs in 2018. Opponents of the program have seized on the PCLOB's review to further argue for closing down the CDR program even though the Board did not find any willful violations of the USA FREEDOM Act, the latter point being likely to be used by proponents of the program.
As noted, even though the House passed the "USA FREEDOM Reauthorization Act of 2020" (H.R. 6172) in early March to reauthorize three expiring Foreign Intelligence Surveillance Act (FISA) provisions, shutter the CDR program and implement reforms, the Senate declined to act immediately on the bill and opted instead to send a 77-day extension of these now lapsed authorities to the House, which is currently in recess. The Senate will turn to a reform bill under a process that will allow votes on specified amendments subject to a 60-vote threshold.

White House Releases 5G Strategy

Last week, the White House released the "National Strategy to Secure 5G of the United States" the same day President Donald Trump signed the "Secure 5G and Beyond Act of 2020" (P.L. 116-129), legislation that requires a 5G strategy the Administration then implements to address the threats posed by a 5G rollout dominated by Huawei and other Chinese companies. Given how detailed the bill was on what must be in the strategy, either this new document is not intended to satisfy this requirement of Congress or it is, in which case a number of lawmakers are not going to be pleased.

The "Secure 5G and Beyond Act of 2020," according to its Committee Report, would:

- Require the President of the United States to develop a Federal Government-wide strategy to ensure the security of the Nation's next-generation—and future generations—wireless telecommunications systems and infrastructure.
- Direct the U.S. Government to assist allies and strategic partners in maximizing the security of next-generation wireless telecommunications systems, infrastructure, and software.

Elsewhere in the report, the Committee explained the legislation "would require the President, in consultation with various other Federal officials, to develop and submit to the appropriate committees of Congress within 180 days of enactment a "Secure Next Generation Wireless Communications Strategy" to do the following:

- Ensure the security of 5th generation (5G) and future generations of U.S. wireless communications systems and infrastructure.
- Provide technical assistance to U.S. mutual defense treaty allies, strategic partners, and other countries, when in the security interests of the United States, to maximize the security of 5G and future generations of wireless communications systems and infrastructure inside their countries.
- Protect the competitiveness of U.S. companies, the privacy of U.S. consumers, and the integrity and impartiality of standards-setting bodies related to 5G and future generations of wireless communications systems and infrastructure."

Moreover, the bill identifies "19 elements that would need to be included in the strategy," including but not limited to:

- A description of U.S. national and economic security interests pertaining to the deployment of 5G and future generations of wire-less communications systems and infrastructure.
- An identification and assessment of the global competitive-ness and vulnerabilities of U.S. manufacturers and suppliers of 5G and future generations of wireless communications equipment. A list of domestic suppliers of 5G and future generations of wireless communications equipment and other suppliers in countries that are mutual defense allies or strategic partners as well as a strategy to assess their ability to produce and supply such systems and infrastructure.
- Identification of trusted supplier entities from both inside and outside of the United States that are capable of producing and supplying to private industry infrastructure and systems equipment supporting 5G and future generations of wireless communications systems and infrastructure.

Additionally, the act requires "[i]n developing the Strategy, the President shall consult with relevant groups that represent consumers or the public interest, private sector communications providers, and
communications infrastructure and systems equipment developers."

In the cover letter, Trump stated

> This National Strategy to Secure 5G articulates my vision for America to lead the development, deployment, and management of secure and reliable 5G communications infrastructure worldwide, arm-in-arm with our closest partners and allies, including:
>
> - Facilitating domestic 5G rollout;
> - Assessing the risks and identifying core security principles for 5G infrastructure;

- Managing the risks to our economic and national security from the use of 5G infrastructure; and
- Promoting responsible global development and deployment of 5G infrastructure.

Trump added

> My Administration is committed to protecting America's national security, promoting our prosperity, and preserving our civil liberties and democratic ideals. Ensuring the security, reliability, and trustworthiness of our 5G infrastructure is essential to these endeavors. This strategy explains how we will do just that.

In the strategy itself, the Administration remarked that "[t]he United States National Cyber Strategy states that:

> The Administration will facilitate the accelerated development and rollout of next-generation telecommunications and information communications infrastructure here in the United States, while using the buying power of the Federal Government to incentivize the move towards more secure supply chains. The United States Government will work with the private sector to facilitate the evolution and security of 5G, examine technological and spectrum-based solutions, and lay the groundwork for innovation beyond next-generation advancements.

The Administration added

> This National Strategy to Secure 5G expands on how the United States Government will secure 5G infrastructure domestically and abroad. 5G infrastructure will be an attractive target for criminals and foreign adversaries due to the large volume of data it transmits and processes as well as the support that 5G will provide to critical infrastructure. Criminals and foreign adversaries will seek to steal information transiting the networks for monetary gain and exploit these systems and devices for intelligence collection and surveillance. Adversaries may also disrupt or maliciously modify the public and private services that rely on communications infrastructure. Given these threats, 5G infrastructure must be secure and reliable to maintain information security and address risks to critical infrastructure, public health and safety, and economic and national security.

The Administration contended that "[t]his National Strategy to Secure 5G will fulfill the goals of the National Cyber Strategy with four lines of effort" identified by the President in his cover letter.

As noted, it is not apparent if this 5G strategy is meant to be the "Secure Next Generation Wireless Communications Strategy" called for in the "Secure 5G and Beyond Act of 2020." And yet, an anonymous Administration official was quoted as saying that the National Strategy to Secure 5G satisfies a part of the bill (without specifying which part) with the implication that the Administration will not be producing a detailed strategy as required by statute. This official also claimed that the implementation plan would be much more detailed.

In any event, the Administration has announced its intention not to fully comply with other parts of the bill. In his signing statement, Trump explained he was going to interpret the new law in ways that would not, in his view, impinge the powers of the President:

- As part of the strategy, section 4 of the Act purports to require the President to engage in international diplomacy in order to share information and pursue policy goals specified by the Congress. Consistent with longstanding constitutional practice, my Administration will treat the relevant provisions of this section in a manner that does not interfere with the President's exclusive constitutional authorities with respect to foreign relations, including the President's role as the sole representative of the Nation in foreign affairs.
- Section 5 of the Act further purports to condition the President's authority to implement parts of the strategy upon the approval of the Federal Communications Commission. My understanding is that this provision does not preclude me or future Presidents from exercising our constitutional authorities as the "sole organ" of the Nation in foreign relations and as the head of the unitary Executive Branch to ensure proper implementation of the entire strategy.

White House Unveils COVID-19 Technology Initiatives

The Trump Administration announced two initiatives that dovetail with existing efforts to broaden the use of big data sets and artificial intelligence and expand U.S. efforts to pioneer the use of the next generation of computing. These efforts tie into the Administration's approach on trying to combat COVID-19.

On March 23, the Trump Administration heralded the formation of the COVID-19 High Performance Computing Consortium which will "provide COVID-19 researchers worldwide with access to the world's most powerful high performance computing resources that can significantly advance the pace of scientific discovery in the fight to stop the virus" per the Administration's statement. The White House explained "[t]his unique public-private consortium, spearheaded by The White House, the U.S. Department of Energy, and IBM, includes government, industry, and academic leaders who have volunteered free compute time and resources on their machines.

U.S. Chief Technology Officer Michael Kratsios asserted "America is coming together to fight COVID-19, and that means unleashing the full capacity of our world-class supercomputers to rapidly advance scientific research for treatments and a vaccine." He thanked the initiatives private sector and academic partners "who are joining the federal government as part of the Trump Administration's whole-of-America response."

In their press release, the Department of Energy contended:

- Researchers are invited to submit COVID-19 related research proposals to the consortium via the online portal which will then be reviewed and matched with computing resources from one of the partner institutions. An expert panel of top scientists and computing researchers will work with proposers to quickly assess the public health benefit of the work and coordinate the allocation of the group's powerful computing assets.
- The COVID-19 High Performance Computing Consortium currently pools 16 systems that together offer over 330 petaflops of supercomputing capacity. Additional capacity, including cloud computing resources, will be added through present and future partners. The sophisticated computing systems available through this Consortium can process massive numbers of calculations related to bioinformatics, epidemiology, molecular modeling, and healthcare system response, helping scientists develop answers to complex scientific questions about COVID-19 in hours or days versus weeks or months.

The White House identified the following private and public sector entities as participating:

Industry

- IBM
- Amazon Web Services
- Google Cloud
- Microsoft
- Hewlett Packard Enterprise

Academia

- Massachusetts Institute of Technology
- Rensselaer Polytechnic Institute

U.S. Department of Energy National Laboratories

- Argonne National Laboratory
- Lawrence Livermore National Laboratory
- Los Alamos National Laboratory
- Oak Ridge National Laboratory
- Sandia National Laboratories

Federal Agencies

- National Science Foundation
- NASA

Earlier in the month, the White House announced "researchers and leaders from the Allen Institute for AI, Chan Zuckerberg Initiative (CZI), Georgetown University's Center for Security and Emerging Technology (CSET), Microsoft, and the National Library of Medicine (NLM) at the National Institutes of Health released the COVID-19 Open Research Dataset (CORD-19) of scholarly literature about COVID-19, SARS-CoV-2, and the Coronavirus group."

The White House added

- Requested by The White House Office of Science and Technology Policy, the dataset represents the most extensive machine-readable Coronavirus literature collection available for data and text mining to date, with over 29,000 articles, more than 13,000 of which have full text.
- Now, The White House joins these institutions in issuing a call to action to the Nation's artificial intelligence experts to develop new text and data mining techniques that can help the science community answer high-priority scientific questions related to COVID-19.
- The collection was constructed via a unique collaboration between Microsoft, NLM, CZI, and the Allen Institute for AI, coordinated by Georgetown University. Microsoft's web-scale literature curation tools were used to identify and bring together worldwide scientific efforts and results, CZI provided access to pre-publication content, NLM provided access to literature content, and the Allen AI team transformed the content into machine-readable form, making the corpus ready for analysis and study.
- The *CORD-19* resource is available on the Allen Institute's SemanticScholar.org website and will continue to be updated as new research is published in archival services and peer-reviewed publications. Researchers should submit the text and data mining tools and insights they develop in response to this call to action via the Kaggle platform. Through Kaggle, a machine learning and data science community owned by Google Cloud, these tools will be openly available for researchers around the world.

EAC Meeting/VVSG 2.0

In conjunction with a public meeting conducted by Zoom, the Election Assistance Commission (EAC) has released for public comment Voluntary Voting System Guidelines 2.0 (VVSG 2.0) Requirements that are "[a]ligned with the VVSG 2.0 Principles and Guidelines," the agency explained in its *Federal Register* notice. The agency explained "the VVSG 2.0 Requirements represent the requirements to which a voting system is tested to obtain certification under the EAC Testing and Certification Program." In the notice of the meeting, the EAC added the VVSG 2.0 are also being shared with the "EAC's Standards Board and Board of Advisors for review." Comments are due by June 22, 2020.

In the VVSG 2.0 Requirements, the EAC's Technical Guidelines Development Committee (TGDC) stated that "[t]he purpose of the guidelines is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems." The TGDC added that "[t]he Guidelines allow for an improved and consistent voter experience, enabling all voters to vote privately and independently, ensuring votes are marked, verified and cast as intended, and that the final count represents the true will of the voters. Federal accessibility standards, Section 508, and Web Content Accessibility Guidelines are referenced and highlighted." The TGDC added that "[v]oter interface requirements have been updated to incorporate recent usability research and interactions that result from modern devices and now fully support accessibility throughout the voting process."

The TGDC the VVSG 2.0 "will be used primarily by voting system manufacturers and voting system test laboratories as a baseline set of requirements for voting systems to which states will add their state-specific requirements as necessary…[and] [t]his audience includes:

- Manufacturers, who will use the requirements when they design and build new voting systems as information about how voting systems should perform or be used in certain types of elections and voting environments.
- Test laboratories who will refer to this document when they develop test plans for the analysis and testing of voting systems as part of the national certification process and state certification testing to verifying whether the voting systems have satisfied the VVSG 2.0 requirements.

The TGDC claimed "[t]his document, therefore, serves as an important, foundational tool that defines a baseline set or requirements necessary for ensuring that the voting systems used in U.S. elections will be secure, reliable, and easy for all voters to use accurately."

The TGDC further asserted

> The cybersecurity of voting systems has never been more important. Indeed, attacks from nation state actors on our elections infrastructure in 2016 led to a critical infrastructure designation. To limit the attack surface on voting systems, the Guidelines require that any election system, such as an e-pollbook or election reporting system, be air-gapped from the voting system. To ensure the integrity of the vote, methods to detect errors through the combined use of an evidence trail and regular audits, including risk-limiting audits (RLAs), compliance audits, and ballot-level audits, are now supported. There is a dedicated section on ballot secrecy, preventing voter information from being carried through to the voting system, and two-factor authentication is now mandated for critical voting operations. Cryptographic protection of data and new system integrity requirements ensure that security protections developed by industry over the past decade are built into

the voting system. These include risk assessment and supply chain risk management, secure configurations and system hardening, exploit mitigation, sandboxing and runtime integrity.

"White Hat" Hackers May Violate Terms of Service In Order To Carry Out Research, Court Rules

A federal court has sided with the Americans Civil Liberties Union (ACLU) and cyber researchers in their case against the federal government, which argued that setting up fake accounts on employment websites looking for bias and discrimination does not violate a federal hacking law. However, the court exercised judicial discretion in declining to rule on the plaintiffs' First Amendment claims. It is unclear whether the Department of Justice will appeal the ruling, or let it stand.

The court summarized the case thusly:

> Plaintiffs are academic researchers who intend to test whether employment websites discriminate based on race and gender. In order to do so, they plan to provide false information to target websites, in violation of these websites' terms of service. Plaintiffs bring a pre-enforcement challenge, alleging that the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §1030, as applied to their intended conduct of violating websites' terms of service, chills their First Amendment right to free speech. Without reaching this constitutional question, the Court concludes that the CFAA does not criminalize mere terms-of-service violations on consumer websites and, thus, that plaintiffs' proposed research plans are not criminal under the CFAA. The Court will therefore deny the parties' cross-motions for summary judgment and dismiss the case as moot.

Elsewhere in the decision, the court stated

> The provision at issue, 18 U.S.C. § 1030(a)(2)(C), or the "Access Provision," makes it a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." Plaintiffs argue that this provision violates the First and Fifth Amendments. Compl. Specifically, they claim that the Access Provision (1) is overbroad and chills their First Amendment right to freedom of speech; (2) as applied to their research activities, unconstitutionally restricts their protected speech; (3) interferes with their ability to enforce their rights and therefore violates the Petition Clause; (4) is void for vagueness under the Fifth Amendment Due Process Clause; and (5) unconstitutionally delegates lawmaking authority to private actors in violation of the Fifth Amendment Due Process Clause. See id. On March 30, 2018, this Court partially granted the government's motion to dismiss. See Sandvig v. Sessions, 315 F. Supp. 3d 1, 34 (D.D.C. 2018). The Court dismissed all but the as-applied First Amendment free speech claim brought by Wilson and Mislove. Id.

Ultimately, however, the court "concludes that agreeing to such contractual restrictions, although that may have consequences for civil liability under other federal and state laws, is not sufficient to trigger criminal liability under the CFAA." The court clariid that "[i]n other words, terms of service do not constitute "permission requirements" that, if violated, trigger criminal liability."

U.N. Group Releases Pre-Draft Report On International Cyber Norms

One of the two United Nations (U.N.) groups convened to address international cyber norms has produced a pre-draft report for comment from all interested U.N. stakeholders, but because of the COVID-19 pandemic, the Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security chair extended the deadline for written submissions to 16 April. The other group, the U.N. Group of Governmental Experts (GGE) has yet to release any such work product. There are important differences between the two groups with the GEE having a termination date and the OEWG not; moreover, the GGE is led by the United States and its allies whereas the OEWG was called for by Russia and the People's Republic of China; and the GGE is limited to 25 members whereas all the nations represented in the General Assembly may take part in the OEWG.

In the fall of 2019, the GGE and OEWG started meeting convened per U.N. resolutions to further consultative discussions on an international agreement or set of agreements on what is considered acceptable and unacceptable cyber practices. Previous efforts largely stalled over disagreements between a bloc led by the U.S. and its allies and nations like China, Russia, and others with a different view on acceptable practices. Notably, unlike 2010, 2013 and 2015, the 2017 U.N. GGE could not reach agreement on additional voluntary, non-binding norms on how nations should operate in cyberspace. The OEWG was advocated for by countries like Russia, the People's Republic of China, and others seen as being in opposition to some of the views propagated by the U.S. and its allies, notably on the issue of what kind of measures a nation may use inside its borders to limit internet usage for its citizens.

As explained in a 2018 U.N. press release, competing resolutions were offered to create groups "aimed at shaping norm-setting guidelines for States to ensure responsible conduct in cyberspace:"

- the draft resolution "Developments in the field of information and telecommunications in the context of international security" (document A/C.1/73/L.27.Rev.1), tabled by the Russian Federation. By the text, the Assembly would decide to convene in 2019 an open-ended working group acting on a consensus basis to further develop the rules, norms and principles of responsible behaviour of States.
- the draft resolution "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (document A/C.1/73/L.37), tabled by the United States…[that] would request the Secretary-General, with the assistance of a group of governmental experts to be established in 2019, to continue to study possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States.

The U.N. noted that '[s]everal speakers pointed out that language in [the Russian proposal] departed from previous year's versions and included excerpts from the Group of Governmental Experts reports in a manner that distorted their meaning and transformed the draft resolution." The U.N. also acknowledged that "some delegates said [the U.S. proposal] called for the establishment of a new group of governmental experts, with the same mandate as the previous ones and the same selectivity in terms of its composition." The U.N. added that "[m]ore broadly, while some delegates regretted to note that two separate, yet similar draft resolutions were tabled, others highlighted a need for bold, swift action to prevent cyberattacks and malicious online behaviour."

Nonetheless, in its pre-draft report, the OEWG made the following recommendations:

a) With regard to international law, reaffirming that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment, the OEWG recommends that:

- Member States be invited to continue to inform the Secretary-General of their views and assessments on Developments in the field of ICTs in the context of international security and to include additional information about national views and practice on how international law applies to State use of ICTs in the context of international security.
- Member States be invited to submit, on a voluntary basis, national views and practice on how international law applies to State use ICTs to the Cyber Policy Portal of the United Nations Institute for Disarmament Research.
- The Secretary-General be requested to establish a repository of national views and practice on how international law applies to the use of ICTs by States in the context of international security.
- The International Law Commission be requested by the General Assembly to undertake a study of national views and practice on how international law applies in the use of ICTs by States in the context of international security.
- *[other recommendations]*
- Member States continue to consider, at the multilateral level, how international law applies in the use of ICTs by States in the context of international security.

b) With regard to rules, norms and principles of responsible behaviour of States, reiterating that voluntary, non-binding norms are consistent with international law, and recalling that in 2015 the General Assembly agreed by consensus that all States should be guided in their use of ICTs by the 2015 report of the Group of Governmental Experts, which sets out 11 voluntary, non-binding norms of responsible State behaviour, the OEWG recommends that:

- Member States be invited to continue to inform the Secretary-General of their views and assessments on Developments in the field of ICTs in the context of international security and to include additional information on their implementation of international rules, norms and principles of responsible behaviour of States in the use of ICTs.
- The Secretary-General be requested to establish a repository of national practices regarding international rules, norms and principles of responsible behaviour of States, which could be further developed into guidance on implementation. The use of surveys or templates on a voluntary basis are encouraged in this regard.
- Further guidance on the implementation of norms of responsible State behaviour be developed and widely disseminated at national, regional, interregional and global levels including through the United Nations. States in a position to contribute expertise or resources to the development and dissemination of such guidance are encouraged to do so.
- *[other recommendations]*
- Member States continue to consider, at the multilateral level, international rules, norms and principles of responsible behaviour of States.

c) With regard to confidence-building measures (CBMs), highlighting that CBMs should be developed and implemented progressively, including at the bilateral, regional and multilateral levels, so as to enhance mutual trust, the OEWG recommends that:

- The Secretary-General be requested to establish a repository of CBMs adopted at regional and sub-regional levels to enable the sharing or exchange of

information on CBMs and identify potential capacity and resource gaps. The repository would be established in coordination with interested regional and sub-regional bodies and without prejudice to further elaboration of CBMs at the global, regional or sub-regional level.

- Members States be encouraged to, on the basis of such a repository, potentially identify the CBMs appropriate to their specific contexts, and cooperate with other States on their implementation.
- The Secretary-General be requested to establish, in coordination with interested regional and sub-regional bodies, a global registry of national Points of Contacts at the policy or diplomatic level, bearing in mind coordination with other such registries, including at the regional and sub- regional levels.
- Member States, which have not yet done so, be encouraged to nominate a national Point of Contact at the policy or diplomatic level, taking into account differentiated capacities.
- Members States be encouraged to explore mechanisms for regular cross-regional exchanges of lessons and good practices, taking into account differences in regional contexts and the structures of relevant organizations.
- *[other recommendations]*

Member States continue to consider CBMs at the bilateral, regional and multilateral levels.

d) With regard to capacity-building, emphasizing its critical functions for empowering all States and other relevant actors to fully participate in the global normative framework, for promoting adherence to international law and the implementation of norms of responsible State behaviour, and for building trust between and within States, the OEWG recommends that:

ICT-related capacity-building efforts in the field of international security should be guided by the following principles:

- *[insert agreed principles]*
- Member States be invited to continue to inform the Secretary-General of their views and assessments on Developments in the field of ICTs in the context of international security and to include additional information on lessons learned and good practice related to capacity-building programmes and initiatives.
- The Secretary-General be requested to establish a global mechanism for enhancing coherence in capacity-building efforts in the use of ICTs, possibly in the form of a facilitation mechanism, in coordination with existing efforts, including at the regional and sub-regional levels. States in a position to contribute expertise or resources to the development of such a mechanism are encouraged to do so.
- Member States be encouraged to further cooperate to build capacity to identify and protect national and transnational critical infrastructure as well as supranational critical information infrastructure.
- *[other recommendations]*

Member States continue to consider capacity-building at the multilateral level.

e) With regard to regular institutional dialogue, affirming that the increasing dependency on ICTs and the scope of threats stemming from their misuse necessitates urgent action to enhance common understandings and intensify cooperation through multilateral discussions, the OEWG recommends that:

- The 76th session of the General Assembly of the United Nations convene a new open-ended working group of the General Assembly acting on a consensus basis to continue the consideration of developments in the field of information and telecommunications in the context of international security.

- States be encouraged to consider establishing sponsorship programmes and other support mechanisms to ensure broad participation. States in a position to support such programmes and mechanisms are encouraged to do so.
- The 76th Session of the General Assembly of the United Nations also consider requesting the Secretary-General to establish a new group of governmental experts.
- *[other recommendations]*

Continuation of National Emergency To Allow For Enhanced Cyber Sanctions

On March 30, President Donald Trump extended for another year the national emergency to combat "significant malicious cyber-enabled activities" put in place initially in 2015 by former President Barack Obama. Trump found "These significant malicious cyber-enabled activities continue to pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States" and therefore warrant an extension for another year. The original executive orders were designed to address hacking and hackers beyond the jurisdiction of the U.S. and were later used to strike back at Russia and its hackers for interfering in the 2016 election. These authorities remain available for use against other nation-states or hacking groups should the Administration choose to use them even though the effect may largely be symbolic against some groups. However, if a commercial entity were sanctioned such as Huawei, lack of access to the U.S. market or to any assets in the country could possibly prove damaging.

In April 2015, in Executive Order 13694, Obama announced his Administration's finding "that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States…[and] I hereby declare a national emergency to deal with this threat." Doing so allowed the Obama Administration to access emergency powers under the following statutes, among others, to take enhanced steps to bring to bear the power of the U.S. government on hackers: the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)). The Administration delegated authority to the Department of the Treasury to block the property of people designated as participating in "cyber-enabled activities" or "trade secrets misappropriated through cyber-enabled means" and other cyber-related activities. Such people would also be subject to a ban on entering the U.S.

In December 2016, in Executive Order 13757, Obama amended the first Executive Order and identified a number of Russian entities and Russian nationals for sanctions related to their interference with the 2016 presidential election, including as detailed in an Obama Administration fact sheet:

- The Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie) (a.k.a. GRU) is involved in external collection using human intelligence officers and a variety of technical tools, and is designated for tampering, altering, or causing a misappropriation of information with the purpose or effect of interfering with the 2016 U.S. election processes.
- The Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB) assisted the GRU in conducting the activities described above.
- The three other entities include the Special Technology Center (a.k.a. STLC, Ltd. Special Technology Center St. Petersburg) assisted the GRU in conducting signals intelligence

operations; Zorsecurity (a.k.a. Esage Lab) provided the GRU with technical research and development; and the Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems" (a.k.a. ANO PO KSI) provided specialized training to the GRU.

- Sanctioned individuals include Igor Valentinovich Korobov, the current Chief of the GRU; Sergey Aleksandrovich Gizunov, Deputy Chief of the GRU; Igor Olegovich Kostyukov, a First Deputy Chief of the GRU; and Vladimir Stepanovich Alexseyev, also a First Deputy Chief of the GRU.

Further Reading

"Exclusive: U.S. officials agree on new ways to control high tech exports to China – sources" – *Reuters*
"Big Tech Could Emerge From Coronavirus Crisis Stronger Than Ever" – *The New York Times*
"Coronavirus pandemic changes how your privacy is protected" – *CNET*
"As Coronavirus Surveillance Escalates, Personal Privacy Plummets" – *The New York Times*
"How Civic Technology Can Help Stop a Pandemic" – *Foreign Affairs*
"U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus" – *The Washington Post*
"How to Think About the Right to Privacy and Using Location Data to Fight COVID-19" – *Just Security*
"Democrats say Google's COVID-19 ad ban is a gift to Donald Trump" – *Protocol*
"Google uses location data to show which places are complying with stay-at-home orders — and which aren't" – *The Verge*
"Leaked Amazon Memo Details Plan to Smear Fired Warehouse Organizer: 'He's Not Smart or Articulate'" – *Vice News*