INSIDE:

Pleased to Meet You
Profiles on the newest group of state CIOs.

Connectivity & COVID-19
How the pandemic has reinvigorated the broadband push.

ON TECH ETHICS

Just because we can, does that mean we should?

PLUS:

The 411 on Text to 911

INSIDE:

Pleased to Meet You
Profiles on the newest group of state CIOs.

Connectivity & COVID-19
How the pandemic has reinvigorated the broadband push.

ON TECH ETHICS

Just because we can, does that mean we should?

PLUS:

The 411 on Text to 911
Faster Smarter Safer

A government executive’s guide to understanding the network of the future and its role in transformative change.

Get your copy at bit.ly/GovFuture
DEPARTMENTS

37 / Seeking Connection
A tidal wave of new virtual learners and remote workers has stretched the capacity of existing Internet options, and digital equity advocates want to capitalize on this renewed interest in their work.

46 / What’s Your Emergency?
Texting rather than calling 911 in an emergency has become increasingly viable, but parts of the country still lack the option.

50 / Privacy and the Law
Some states seek to emulate California’s sweeping though yet-to-be-enforced digital privacy legislation, while action stalls on the federal level.

COLUMNS

4 Point of View
New leaders take the reins at the state level.

7 Data Points
COVID-19 may speed government’s use of virtual reality tech.

8 Four Questions
Acting New York CIO Jeremy Goldberg on the transition from city to state IT.

56 CIO Street View
Chief information officers will be key to moving toward a new normal.

58 Cybersecurity Strategies
Answering tough questions in a crisis.

NEWS

6 govtech.com/extra
Updates from Government Technology’s daily online news service.

10 Big Picture
Supercomputers use AI to search for a coronavirus vaccine.

52 CIO Central
Career changes across tech-driven roles in local government.

54 Products
Lenovo Mirage VR S3 headset, FUJITSU LIFEBOOK U7310, Dell Precision Compact Workstation.

57 Spectrum
More research, more science, more technology.

IN OUR NEXT ISSUE:

Cloud Clarity
Has “going to the cloud” delivered on its promise?

Gender Gap
A look at the push for more women in government IT.

Survey Says
Percentages and projections on government cloud adoption.

COVER STORY

12 / Second Look
The pandemic boosted the credibility of some newer technologies. Will a newfound open-mindedness last?

32 / In the Balance
As automation becomes an ever-more viable tool for government, can policymakers ensure it is used responsibly and ethically?

40 / The New Class
Twelve new state chief information officers step into the role during unprecedented times.

32 / In the Balance
As automation becomes an ever-more viable tool for government, can policymakers ensure it is used responsibly and ethically?

40 / The New Class
Twelve new state chief information officers step into the role during unprecedented times.

32 / In the Balance
As automation becomes an ever-more viable tool for government, can policymakers ensure it is used responsibly and ethically?

40 / The New Class
Twelve new state chief information officers step into the role during unprecedented times.

32 / In the Balance
As automation becomes an ever-more viable tool for government, can policymakers ensure it is used responsibly and ethically?

40 / The New Class
Twelve new state chief information officers step into the role during unprecedented times.

32 / In the Balance
As automation becomes an ever-more viable tool for government, can policymakers ensure it is used responsibly and ethically?

40 / The New Class
Twelve new state chief information officers step into the role during unprecedented times.

32 / In the Balance
As automation becomes an ever-more viable tool for government, can policymakers ensure it is used responsibly and ethically?

40 / The New Class
Twelve new state chief information officers step into the role during unprecedented times.
In Capable Hands

In the last 12 months, a dozen new state CIOs have been named. And what an environment these tech leaders have entered, some literally in the throes of a global pandemic that tested the capability and flexibility of state technology systems like never before. Of the tech leaders we profile in The New Class, p. 42, seven assumed the role in early 2020, many in March, the month when the country’s first stay-at-home orders were issued.

In May, the country endured 100,000 fatalities from the novel coronavirus—a grim milestone that seemed inconceivable as the calendar turned to 2020. And while state leaders were rightly focused on the health, safety, and well-being of their communities, they also grappled with how to maintain the operations of critical government services. If governors weren’t closely acquainted with their top technology officials before the outbreak, it’s safe to say they are now.

This group brings a diverse set of work and life experiences to their roles as state CIOs—breadth that will serve them well as they look to navigate unprecedented circumstances. North Carolina’s Tracy Doaks now finds herself in a more public-facing role, after having served for four years as a more back-office technologist as deputy CIO for the state.

“No my focus has expanded to all facets of the Department of Information Technology,” Doaks explained, “so that includes cybersecurity, data analytics, rural broadband, 911, digital transformation.”

Similarly, Iowa’s Annette Dunn—a veteran among this group, having been named CIO in August 2019—notes similarities between her prior role as CIO of the state’s Department of Transportation and her statewide position, albeit on a bigger stage.

By now, they’ve transitioned their workforces to enable remote productivity and brought them back to the office again, though perhaps not as many as pre-pandemic. They will continue to play a critical part in navigating what both onsets and virtual work environments need to function.

And then they’ll need to confront the pivot back toward essential technology upgrades that were put on the back burner in order to address more pressing issues. As the economy begins to recover from mass closures, government budgets will suffer severe shortfalls, forcing plans to be re-evaluated. This will add layers of complexity to their work.

“We’re looking at precipitous declines in revenue over the next six, 12, 18 months,” said Michigan CIO Brom Stibitz, who took the helm in March 2020 following five years of tech leadership for the state. “So there’s going to be more pressure than ever on IT to (a) find efficiencies within that which we’re doing, and (b) to find solutions that can help agencies or customers save money.”

They will need to draw upon their passion for public service in order to successfully communicate priorities and jockey for needed resources in an environment with previously unseen constraints.

But many have noted what new Missouri CIO Jeff Wynn described as a “silver lining in a very dark cloud” of COVID-19. The pandemic has helped expedite plans for IT transformation and modernization, and proved just how impactful those efforts can be. Missouri’s IT group quickly set up chatbots to help deal with an influx of citizen inquiries and partnered on a “match-making” project of sorts to pair PPE suppliers with the needs of healthcare organizations. Further, IT upgrades were carried out quickly to meet pandemic-related needs.

We will be following the work of this new class of state CIOs closely, both on the pages of this magazine and with our daily reporting at gotech.com. The challenges they face are great, but they stand ready to meet them and press forward with modernizing their infrastructure and workforce for the challenges that lie ahead.

By Noelle Knell / Editor
Preparing state & local leaders for the new normal

2020 brought new uncertainties that required state and local agencies to rapidly shift to a new normal for their work and operations. Thriving in the new normal requires a future ready foundation that intelligently connects people, processes and technology.

You can learn how to prepare for this new normal with actionable resources and best practices at govtech.com/futureready.

FutureReady Hub Resources

Stories from the Trenches – learn how state and local agencies and Google are working together on COVID-19 response and building platforms ready for whatever is ahead.

COVID-19 Community Mobility Reports – learn what has changed in response to work from home, shelter in place, and other policies aimed at flattening the curve of the pandemic.

Modernizing Social Safety Net – learn how to create a one-stop-shop to modernize the most vital government social systems.
**Distance Learning**

A six-hour course from the Johns Hopkins Bloomberg School of Public Health, available for free on the online learning website Coursera, offers training to anyone interested in contact tracing, which health officials say is critical to stopping the spread of the coronavirus. Skills taught include how to interview people with the virus and identify their close contacts who may have been exposed.

**NO WAIT**

In a well-timed rollout, Vermont launched its online driver’s license renewal platform just as shelter-in-place orders were given. While the Department of Motor Vehicles was closed in response to the novel coronavirus, residents no longer had to make in-person DMV visits anyway. The move is part of a comprehensive modernization aimed at making drivers’ licenses more secure. Licenses are now being produced off-site by a company called Valid, which also offers a platform allowing Vermonters to do more transactions remotely.

**Biz Beat**

After two-and-a-half years, Alphabet subsidiary Sidewalk Labs announced it was ending work on its controversial Waterfront Toronto project. Sidewalk Labs CEO and founder Daniel Doctoroff attributed the decision to economic impacts of COVID-19. The project’s aim was to build a sustainable, smart community in the Canadian city.

**WHO SAYS?**

“We’ve shifted from commuting to computing. And that’s a huge permanent change. And there’ll be a lot of resistance to go back to the way before.”

govtech.com/quotejuly2020

**MOST READ STORIES ONLINE:**

- Oklahoma Takes On Mass Unemployment Through New Platform
- Cyberattack Disrupts Texas Department of Transportation
- Arkansas Shuts Down Unemployment Website After Data Exposure
- The Pandemic Will Mean Big, Lasting Changes for Urban Mobility
- Four States Share Realities of the Transition to Telework
- Five Takeaways from State CIOs on Pandemic Response
The Future Is Immersive

The pandemic may accelerate the use of virtual and augmented reality technology by state and local government.

With the staff of many government agencies forced to work from home because of COVID-19, government CIOs have had to move quickly to adapt. While the initial focus has been on ensuring workers have the basic tools they need to do their jobs — fast and secure Internet, laptops and mobile devices, and access to essential online systems — as weeks turn into months, more government agencies must start exploring opportunities for better remote collaboration, communication and training. One opportunity on the horizon is expanding the use of immersive computing technologies, like augmented reality and virtual reality (AR/VR), that create new modes for users to experience digital content through computers, mobile devices and headsets.

There are some immediate ways that government can use AR/VR, such as to improve training for workers. AR/VR lets agencies simulate real-world situations, giving workers the opportunity to gain experience in a controlled environment. This type of training is particularly useful for law enforcement and other first responders who encounter situations where there can be severe consequences from mistakes made during on-the-job training. Learning in an AR/VR environment has been found to not only increase recall, but also allow trainees to develop muscle memory for specific tasks. And perhaps most importantly, AR/VR may also be the most feasible option for remote training for workers at home or who cannot travel and would otherwise be unable to attend onsite training.

AR/VR can also be useful for recruiting prospective employees. For example, the Indiana Department of Child Services reduced its 50 percent annual turnover in case workers to 17 percent by implementing a VR simulation that gives job applicants better insight into what their daily job duties would entail. At the federal level, the Marine Corps began exploring earlier this year how the use of head-mounted VR simulators might improve recruiting, particularly among college students, after its past successes using flight simulators.

Immersive computing may also help government agencies better engage with the public. Cities like Boston and Seattle have already piloted using various forms of AR/VR to help city planners, elected officials, citizens and others better engage in community planning. Instead of just looking at basic 2-D design plans, AR/VR can enable individuals to interact with 3-D models or virtual video simulations, thereby allowing them to better understand what a new development might look like or the impact it would have on traffic patterns. As more communities invest in smart city technology and generate significantly more data, AR/VR applications may become one of the primary ways of visualizing this information.

Finally, cities can also produce AR/VR content for the public, which may prove especially useful in a post-COVID-19 world. Museums have been early adopters of this technology as they let visitors experience virtual exhibits even when museum facilities are closed. And cities, such as New Orleans, have also created virtual tours, allowing would-be tourists to, for example, experience the French Quarter and learn more about the city’s history and culture.

And AR mobile apps not only provide enhanced navigation, such as showing pedestrians walking routes, but they can also layer on additional content such as information about points of interest. Such apps can not only deliver more information, but also create more touchless encounters, like replacing shared paper menus at restaurants with virtual ones.

The eventual goal of many AR/VR developers is to allow for virtual meetings. While many more people are now using video conferencing, complaints are already stacking up about how it fails to sufficiently replicate the in-person experience. AR/VR technology is not yet ready or widely adopted enough for this type of collaboration to be mainstream, such as for VR town hall meetings, but the ability to have small teams collaborate in a virtual environment is starting to be deployed. Some cities are seizing this opportunity. In 2018, New York City established RLab, the first publicly funded AR/VR facility to support economic development, academic research and entrepreneurship.

Not every city can or should follow in its footsteps, but there are a number of potential applications of AR/VR in government, and the timeline to adopt these technologies has likely been accelerated by the pandemic. Agencies should use this opportunity to begin planning for, and piloting, this new technology.
Jeremy Goldberg describes himself as a “student of civic tech and gov tech.” His resume includes time with San Francisco, where he helped launch the Startup in Residence (STiR) program, as well as three years as New York City’s deputy CTO. Since November 2019, Goldberg has been acting CIO for New York state, a position that’s both broader than and similar to his city-level work.

1 How has your experience in major cities translated to state work?
San Francisco prides itself on being the center of the tech industry, and that’s clearly played a role in both the access to and engagement with technology and technologists. Tech certainly has a strong presence in New York City, but you can’t say that New York is defined by the tech industry the same way as San Francisco. Technology is a part of every industry in New York, from the arts and academia to finance and banking, and that has influenced the city government’s approach to technology. The approach to gov tech over the last decade speaks to the importance of these regional differences.

Still, the state level is different in some critical ways. New York has a 50-mile drone corridor that stretches from central New York to the Mohawk Valley. We have a thriving biotech industry in the capital region, and about 20 percent of the state’s land area is used for farming and has benefitted tremendously from ag-tech solutions. The other important part from the state perspective is the ability to coordinate and direct the state’s resources and our technical knowledge at scale. That’s been a major boon for just about every area of the state, and that’s something that can’t quite be replicated at the city level.

2 Do civic tech efforts like the STiR program work at the state level?
Over the past 10 years, a lot of cities really have been leaders in the gov tech or civic tech space. And we’ve begun to see that many of their lessons are making their way into state government at this time, including here in New York where we have the resources to scale that work and make it successful for the entire population. I see increasingly a growing leadership role for state government and governors in charting a course for the next 10 years of civic tech.

3 How will the COVID-19 response affect New York state long term?
We know the crisis is having a very severe economic impact, and that means that we need to use our resources even more efficiently and effectively. It’s not just about policy, it’s about operational approaches and priorities. The old model of “buying more stuff” to solve our technology problems won’t be financially viable any longer, but the crisis has also reinforced the lesson that it also wasn’t going to be technologically viable. So we have to be smart, thoughtful and agile in the way we approach technology across the board, and if we are, we have an opportunity for positive and transformative change.

The state’s response to the coronavirus has also reinforced the need for flexibility and stability across the state’s technology infrastructure and workforce. By “flexibility” I mean that we can shift our focus to respond to a crisis or a new priority at a moment’s notice. The stability piece is so our services remain reliable during normal operations so we can continue to be resilient as we face unprecedented events, and we’re really taking proactive steps to support our technical workforce with the technologies and training that they need.

4 What does that workforce development look like?
We’re working closely with our human resources team, expanding access to professional development and training opportunities and promoting employee engagement. We’re going to be doing this not only for the Information Technology Service workforce, but also offering them up to digital information officers and others across the state, helping to equip them with new tools to operate more effectively in a digital environment. It’s putting the people and process in place before the technology.

— Lauren Harrison, Managing Editor
SPREADING BEST PRACTICES & SPURRING INNOVATION IN CHALLENGING TIMES.

DIGITAL GOVERNMENT SUMMITS ARE GOING VIRTUAL!

ATTEND/SPONSOR:
govtech.com/events
Two rows of Frontera supercomputer servers at the Texas Advanced Computing Center.
In response to the pressing need for a vaccine or drug to slow the spread of or heal those infected with the novel coronavirus, research teams are harnessing the power of supercomputers, using artificial intelligence to evaluate every molecule that might possibly interact with the virus and look further into those that seem most promising. Many of those computers, including the Frontera (pictured) at the Texas Advanced Computing Center at the University of Texas at Austin, funded by the National Science Foundation (NSF), are running through millions of simulations as they work to quickly identify candidates to combat COVID-19. More than 30 teams worldwide are together undertaking work that would not otherwise be possible in the timeline the aggressive virus necessitates, the NSF reports.

SOURCE: NATIONAL SCIENCE FOUNDATION

A worker builds a station onsite that supports the power for the Frontera supercomputer.
The onset of the novel coronavirus forced many who were reluctant to embrace technology into Internet-dependent remote work environments, virtual meetings and even to government websites in numbers never before seen. Chief information officers in state and local government that GT has interviewed over the past few months predict that the traditional way of working that tethered staff to physical buildings will never return. Maryland CIO Michael Leahy said in a virtual NASCIO panel in May that he’s seriously considering making the switch to telework permanent for all state IT personnel. So while the pandemic was most definitely unwelcome, it forced open some minds that had previously been closed to technology’s potential.

But will this wave of good feelings extend to other nascent technologies that aren’t fully mainstreamed? The past few years have brought unwelcome revelations about the practices of some big technology companies whose business models depend on trading in personal data many of its users didn’t realize was being collected. And many Americans still fear widespread use of Big Brother-style surveillance technologies. But the crisis prompted a new acceptance of experimentation in the name of protecting public health. While we don’t yet know whether these small-scale uses will become permanent, they at least provided a chance for a close look at their potential in practice.

Here, we look at recent deployments of a handful of emerging technologies called into service because of COVID-19.

The pandemic boosted the credibility of some newer technologies. Will a newfound open-mindedness last?

By GT Editorial Staff
When COVID-19 began sweeping across the country earlier this year, thermal camera and sensor vendor FLIR Systems began marketing its products as a way to help screen people for fevers. The cameras, which can read heat signatures on people and objects, have traditionally been used in industrial and military settings, but FLIR believes they could be used to help organizations navigate the pandemic and evaluate illness.

“We’ve just seen an immense uptick in interest since all this started,” said Chris Bainter, global business development director with FLIR, discussing the global interest from public and private organizations alike. Evidence that the tech is gaining traction, the company installed its temperature screening system at the Pentagon Visitor Center in early June.

FLIR is not alone. Thermal cameras are seeing an industry boom, and many other security firms across the globe have begun marketing their products as potential tools to deploy against the spread of illness.

Since the pandemic hit, sales have been brisk for Athena Security, said CEO Lisa Falzone, which recently launched its Fever Detection COVID-19 Screening System.

Much of this buying has been going on in the private sector. According to Bainter, his company has recently developed contracts with restaurant owners, grocery stores, events vendors and others. Similarly, Falzone said her company has seen interest from all over: hospitals, 911 call centers, airports and more.

“The orders are coming in from all walks of life, businesses large and small that want a pre-screening technology in place,” she said in an email.

However, these cameras don’t detect the virus itself; they merely measure whether a person has an elevated skin temperature or not. This means that they aren’t a catch-all solution, but rather, could be integrated into a broader public health and safety process involving screening and diagnosis.

Hypothetically, these devices could have many uses for governments. City halls could identify sick staff before they entered a building; airports could screen passengers to cut down on the likelihood of national or international carriers; and jails and prisons might be able to prevent an outbreak before it occurs.

In other parts of the world — such as Europe and large parts of Asia — this is already taking place. There, thermal imaging systems are paired with other tech like facial recognition, movement predictive algorithms and data tracking to help contain the virus.

At the pandemic’s ground zero, in Wuhan, China, transportation hubs recently began rolling out a thermal imaging system created to spot people with fevers. This system, designed to set off an alert when an individual’s temperature rises above 37 degrees centigrade, also has an AI-driven facial recognition component that can identify specific individuals.

For obvious reasons, federal or municipal deployment of such technology can be problematic. Many countries are using thermal imaging systems to identify elevated temperatures that could indicate someone is sick with COVID-19, but U.S. watchdog groups are concerned about privacy implications.
in the U.S. has had its detractors, and civil liberty activists worry that the tech goes too far in its pursuit of safety.

The Electronic Frontier Foundation (EFF) published a statement earlier this year on thermal cameras, questioning the accuracy of the technology, and arguing that the surveillance infrastructure being built up now might become permanent even after the virus goes away.

"After 9/11, we got the Patriot Act," said Matthew Guariglia, policy analyst with EFF. "A lot of times [after a large event] the initial public safety concerns allow people to ignore or disregard the long-term civil liberties implications, because of the initial panic. Terrorism is one thing — because it’s an ongoing problem. But there’s no reason why this kind of technology would need to stick around after the COVID-19 crisis is over.”

CELLPHONE LOCATION DATA

In late March, the Kansas Department of Health and Environment (KDHE) announced it was using a “Social Distancing” dashboard recently launched by Unacast, a location data and analytics firm, that uses phone GPS data to illustrate the spread of the virus. The data, which is anonymized and aggregated, showed at a county level how effectively residents were abiding by local stay-at-home orders. Updated daily, the dashboard synthesized data from a number of sources, according to a company representative. The dashboard also graded communities on how well they practiced social distancing and stayed away from “non-essential” outdoor venues, like stores, hotels and restaurants.

“We have to uniformly, across the state of Kansas, get serious about this to decrease the amount of travel we’re doing and stay home,” said Dr. Lee Norman, the head of KDHE, at a joint press conference with Gov. Laura Kelly.

And while this type of tracking technology has been somewhat controversial, Ashley Jones-Wisner, senior director of public affairs with KDHE, said that the platform was merely a means of showing whether people were mostly following the containment orders.

“Cellphones’ Social Distancing Scoreboard shows the change in the number of “human encounters” in Manhattan from Feb. 26 (left) to March 24.”

“There are essential services and actions allowable under the Stay at Home order. The data, as indicated in the [Unacast] methodology section, takes that into account but looks for overall reduction,” she said.

By late May, all 50 states had begun reopening, with many variations on phased approaches appropriate to local circumstances. How to safely and fully reopen economies is a question on everyone’s mind, and a consensus is forming: Experts don’t believe governments and businesses can safely reopen without wide-scale testing and tracing.

To that end, some researchers at the Massachusetts Institute of Technology (MIT), and separately at companies such as Apple and Google, are designing apps to help fill that role.

MIT’s Safe Paths platform uses GPS and Bluetooth to log people’s locations in a secure diary, so if they wind up testing positive for the coronavirus, they can provide health officials with a record of where they’ve been. Health officials can then use the Web app to redact personally identified information.

“Second Look”

www.govtech.com // July/August 2020

15
identifiable information from the location trail and release the information to the public, so other people can look up — or even get automatic notifications — if they recently crossed paths with any carriers.

SafePaths is open source and interoperable with similar apps, and both are crucial to build the knowledge base needed to reopen the economy, according to MIT project lead and Associate Professor Ramesh Raskar. Absent an organized federal test-and-trace program, state and local governments will need to acquire that information themselves.

Apple and Google announced in April that they’re working on a similar software kit, and released application programming interfaces (APIs) in May that allow interoperability between Android and iOS devices using apps from public health authorities. In the coming months, both companies will release a broader Bluetooth-based contact tracing platform: “a more robust solution than an API [that] would allow more individuals to participate, if they choose to opt in, as well as enable interaction with a broader ecosystem of apps and government health authorities,” according to the announcement.

Similar contact tracing mobile apps are underway around the world: In Europe, Pan-European Privacy-Preserving Proximity Tracing is developing a scalable, interoperable software system for mobile-based contact tracing; in Singapore, the government used a tool called TraceTogether; in Hong Kong, it was called StayHomeSafe.

In short, contact tracing in the United States and around the world will be a team effort. MIT said it’s working in various capacities with people from Harvard, Stanford, State University of New York at Buffalo, Mayo Clinic, Massachusetts General Hospital, the World Health Organization, the U.S. Department of Health and Human Services, and the Graduate Institute of International and Development Studies; as well as with experts from governments and institutions in Canada, Germany, India, Italy, the United Kingdom and Vietnam.

Above all, Raskar was adamant that contact tracing will still require interviews and organized work from public agencies, in addition to data yielded by mobile apps and software platforms.

“We think that manual contact tracing by public officials is a very important piece of the puzzle. We don’t think this problem can be solved purely by a piece of software,” he said.

DELIVERY ROBOTS

The COVID-19 crisis also seems to be jettisoning real-world uses of autonomous technology. In a recent example, wheeled robotic cargo devices began delivering food from restaurants in Virginia. Starship Tech-
Technologies deployed a fleet of 20 autonomous "on-demand robots" in April in Fairfax, Va. The devices deliver food and groceries from a handful of restaurants and markets in and around the small city's downtown area. The robots travel via city sidewalks and move about 4 mph, making short-distance deliveries within a radius of a few miles, according to the company. The devices are controlled remotely, can travel in rain or snow, and have human operators ready to take over. "We like to frame ourselves as being very innovative and forward thinking when it comes to trying new things to help grow our local economy. And so, this had been on my radar, but it really bubbled to the top," Fairfax Economic Development Director Christopher Bruno said in April.

The autonomous devices have separate insulated areas for hot and cold items, and are equipped with cameras, sensors and other technology to help them glean traffic patterns, curb-cuts and other information about the built urban environment.

"They're able to take food from restaurants and deliver it to the front door of residents that are ordering food through their app," said Bruno. "There's no better time to be trying something like this, in a time when we're discouraging human contact," he added.

Users must download the Starship app, where they can select and order items, and then set where the order should be delivered. Shoppers can also follow the vehicle ferrying their goods via an icon making its way across a map of the area. When the robot arrives, shoppers receive an alert, and then unlock the device via the app. Starship operates in five countries, and has mostly traveled across college campuses in the United States to date. Its devices have logged 100,000 commercial deliveries, traveled 500,000 miles and crossed 5 million streets around the world as of June 1, according to company officials.

Starship has recently launched a similar service in Mountain View and Irvine, Calif.; Tempe, Ariz.; and Washington, D.C. Autonomous technology was also recently put to work in Florida, where small autonomous shuttles are used to transport COVID-19 tests at the Mayo Clinic. And Refraction AI began testing its small autonomous delivery vehicles in Ann Arbor, Mich., more than a year ago. The coronavirus crisis has rattled the lives of residents and businesses worldwide, as local governments scrambled to assemble rescue and other aid measures for local businesses. A project to launch a fleet of robot delivery vehicles would normally take months to plan and deploy, said Bruno, but it was expedited in light of the urgency brought on by the pandemic. "We're essentially pulling this together in a little under two weeks," Bruno said.

DRONES

Within weeks of the outbreak hitting the U.S., drones became a tool for local police departments looking to help control COVID-19 cases in their communities. The most common use case appears to be utilizing the machines to reinforce social distancing rules. If a crowd gathers in a public area, an officer will deploy a drone that will, via loudspeakers and a recorded message, urge citizens to disperse. This method has been used in countries like China and Spain. According to multiple sources in the Elizabeth Police Department in New Jersey, officers were seeing public crowds daily, whether on street corners, in play areas or in public streets.

"The practical reasoning is that a drone can cover more ground and have a greater advantage point over officers on the ground," according to the department. "It also facilitates in assisting patrol in getting to hard-to-reach areas. Officers can patrol remote areas without leaving their vehicle area. PSAs can be delivered in public places without the danger of officer contact."

Keturah Greene, public information coordinator for the Savannah Police Department in Georgia, cited similar reasoning.

"Since utilizing various strategies such as placing a sign board with social distancing messaging in a popular park which is usually highly populated, utilizing the drones and by educating the community through social media,
In its statement, the Elizabeth Police Department said the PSAs aren’t delivered by drones for “surveillance purposes.” The department also referred to legal precedent.

“There’s been plenty of case law on how this does not infringe on citizens’ rights,” the email read. “Florida v. Riley held that police officials do not need a warrant to observe an individual’s property from public airspace.”

Lt. James Munro, who works for the Clovis Police Department in California, said his department won’t be using its drones to issue social distancing messages to crowds. Munro added that Clovis always takes a cautious approach, only using drones when necessary and being mindful of the public’s trust.

“It would make more sense to use a patrol car [to issue PSAs],” Munro said. “You can cover more ground faster. With drones, you have to have line of sight.”

The Elizabeth Police Department indicated to Government Technology that it’s looking into using drones to map our future COVID-19 test sites, monitor such sites and assist emergency medical technicians. Two factors may continue to drive more drone use during the pandemic. First, the Federal Aviation Administration issued an update titled “Drone Use for COVID-19 Response Efforts” on April 14. With this update, the organization opened the door for drone transport of goods and “certain medical supplies,” as well as expedited approvals for “flights that support emergency activities and appropriate government, health or community initiatives.”

Second, Chinese drone manufacturer DJI announced its Disaster Relief Program in late March. As part of the emergency program, DJI has sent 100 drones to public safety agencies in almost half of all states. Munro said he sees drones becoming even more important for police work in the future. “Drones [are] one piece of technology that, as a police agency, I don’t think we could live without anymore,” Munro said. But drone use in response to COVID-19 has had controversy. Police in Westport, Conn., thought they had found a viable method to monitor whether citizens showed signs of COVID-19 infection in the form of a new drone, but public comments inspired the local department to abandon the technology.

The Police Department in Westport decided against participating in the “Flatten the Curve Pilot” two days after announcing its intention to test new drone technology from Dronefly. According to a news release from Dronefly, the drone uses a “specialized sensor and computer vision systems” that can detect fever, measure heart and respiratory rates, and identify whether people are coughing, sneezing or practicing social distancing. The drone can reportedly do all of this from up to 190 feet away.

According to the press release announcing the Westport project, such drones wouldn’t be used around private yards, but they would help monitor “beaches, train stations, parks and recreation areas, and shopping centers.”

Westport Police Chief Poti Kuskinas said COVID-19 has ushered in an age where drones need to be utilized for public safety. The department confirmed to GT that it wanted to be transparent about its intention to use Dronefly’s drones, with the expectation that the public would make its feelings known upon learning about the program. Amid both positive and negative feedback, the agency canceled the project.

One organization speaking out in opposition was the Connecticut chapter of the ACLU.

“Any new surveillance measure that isn’t being advocated for by public health professionals and restricted solely for public health use should be promptly rejected,” said David McGuire, executive director of ACLU of Connecticut, as reported by the Hartford Courant. “And we are naturally skeptical of towns announcing these kinds of partnerships without information about who is operating the drones, what data they will collect, or how, or if that data will be stored, shared or sold.”

Despite the setback for Dronefly, CEO Cameron Chell told VentureBeat that the company has two more pilots lined up. And though both pilots would be in the private sector, Chell cited interest from others in the public sector, and remarked that initial testing in Westport showed promise.
Best of What’s New in Data, Identity and Privacy

Navigating a sea change in data management and compliance.
In May, Kansas Attorney General Derek Schmidt sent a letter to the governor and the state legislature urging them to create a new legal framework to guide the use of contact-tracing data intended to reduce the spread of COVID-19.

Schmidt said new software tools that use cellphone location data to alert individuals when they come in contact with someone who has tested positive for the coronavirus are “certain to present challenging legal issues not addressed by current Kansas law.”

Schmidt isn’t the only one raising concerns. The urgent public health requirement to track and limit exposure to the highly contagious virus has sparked growing worries that aggressive surveillance techniques threaten privacy protections for patient medical records.

“All of this is occurring without even a basic statutory architecture to guide development and deployment of the practice and management of the sensitive personal information collected,” Schmidt wrote to Kansas Gov. Laura Kelly and legislative leaders.1

COVID-driven tensions turn up the heat on an issue that’s been simmering for several years. Massive technology-enabled growth in the collection and monetization of personal data has sparked pushback in the form of legislation intended to give citizens more control over how organizations collect, use and protect information about them.

State lawmakers across the nation introduced hundreds of privacy bills just last year. One of the most prominent pieces of 2019 privacy legislation — the California Consumer Privacy Act (CCPA) — took effect in January, marking the first of potentially many state-level attempts to emulate the European Union’s groundbreaking General Data Protection Regulation (GDPR), which gave EU residents more control over how organizations use their personal information.

New Privacy Expectations

All of this points to a sea change in how state and local government agencies must manage and protect data. The societal shift toward reasserting privacy as a fundamental right is driving heightened citizen expectations for government agencies to be responsible stewards of personal information. It’s also reshaping the regulatory environment for public and private sector organizations.

“Government organizations are going to have to demonstrate the ability to discover and identify protected data — and map how that data is used,” says Deb Snyder, former chief information security officer for New York State who is now a senior fellow with the Center for Digital Government (CDG). “Agencies need these capabilities to instill citizen confidence and demonstrate compliance with new regulations. It’s essential for them to know what data they have, where it resides, who accesses it and what business processes it supports.”

That’s easier said than done. Governments have spent the past 30 years creating a patchwork of interconnected systems that share data to support transactions and business processes. Unfortunately, the touchpoints and data flows between these systems often are poorly mapped, making it difficult to understand how and where data is used. And demonstrating compliance with multiple regulatory requirements across this uncertain terrain is even harder still.

“It creates insane complexity,” says Snyder. “You need the ability to map all of that and then apply a set of controls to it. You also need to demonstrate and confirm continuous compliance by monitoring those systems and policy settings in real time.”

SPONSORED CONTENT

Understanding the New Privacy Landscape

Discover and identify protected data — and map how that data is used — says Deb Snyder, former chief information security officer for New York State who is now a senior fellow with the Center for Digital Government (CDG). “Agencies need these capabilities to instill citizen confidence and demonstrate compliance with new regulations. It’s essential for them to know what data they have, where it resides, who accesses it and what business processes it supports.” That’s easier said than done. Governments have spent the past 30 years creating a patchwork of interconnected systems that share data to support transactions and business processes. Unfortunately, the touchpoints and data flows between these systems often are poorly mapped, making it difficult to understand how and where data is used. And demonstrating compliance with multiple regulatory requirements across this uncertain terrain is even harder still.

“It creates insane complexity,” says Snyder. “You need the ability to map all of that and then apply a set of controls to it. You also need to demonstrate and confirm continuous compliance by monitoring those systems and policy settings in real time.”

...
Results from CDG’s annual Digital Cities and Digital Counties surveys indicate CIOs are feeling the impact of these data management issues. Technology governance ranked among the top 10 technology priorities for city and county respondents in 2019. In addition, chief privacy officers (CPOs) — charged with managing risk, creating privacy policies and ensuring compliance with its public privacy laws — are becoming more common in state and local governments. Thirty-six percent of cities and 45 percent of counties have at least one full-time position dedicated to enterprise privacy responsibilities, according to the 2019 surveys. And at least 13 states have created a CPO or similar position, according to a 2019 Government Technology report.

Smart Tools for Compliance
Fortunately, technology tools available to help governments address privacy challenges are growing smarter and more sophisticated. For instance, data discovery tools can help agencies understand where sensitive data is stored and how it is used by various systems. In addition, intelligent risk management solutions use artificial intelligence and machine learning to continuously monitor compliance with security and privacy requirements across complex IT environments.

Importantly, these and other data management technologies also can extend to data used by cloud service providers and third-party contractors.

“Trend organizations are going to have to get serious about service providers and hold them to the same compliance requirements,” says Snyder, “which can span from reviewing contracts and updating procurement procedures to automated reviews of systems that are beyond the immediate reach of the organization.”

Ultimately, these tools help agencies get a better handle on what data is most critical to business processes and/or most sensitive from a regulatory perspective, so they can apply the right level of protection.

“If you don’t know those basics, it’s hard to properly focus your resources on bringing things into compliance or to a better state,” she says. “You’re just basically shooting in the dark.”

Snyder adds that agencies should limit the amount of citizen data they gather and maintain. “Try to collect only as much data as you need to perform a specific function, and routinely purge data you no longer use,” she says. “The more you keep, the greater your possible risk and exposure.”

Get Started
As citizen expectations continue to rise and the regulatory landscape grows more complex, agencies must commit to strengthening their privacy programs. Classifying data, mapping information flows, and implementing smart compliance and risk management tools will all be part of this effort.

“The message really is just get started,” says Snyder. “Being able to protect privacy and prove compliance isn’t optional.”

GROWING ATTENTION ON PRIVACY

| 45% of counties have a full-time position dedicated to enterprise privacy responsibilities. | 36% of cities have a full-time position dedicated to enterprise privacy responsibilities. | 13 states have appointed a chief privacy officer or similar position. |

Data governance ranked #6 in the top 10 technology priorities for city and county CIOs.

SOURCE: 2019 DIGITAL CITIES AND COUNTIES SURVEYS AND GOVTECH.COM

*https://www.govtech.com/policy/Kansas-AG-Calls-for-Contact-Tracing-Limits-Privacy-Protections.html
Protecting the Data That Matters Most

Tony Encinias, chief strategy and innovation officer, state and local government for Dell Technologies, and former CIO of the commonwealth of Pennsylvania, shares best practices to simplify data protection and compliance.

What are the challenges of protecting personal information and complying with new data privacy laws?

For one, organizations must find funding for technologies that can meet the requirements of new legislation. In addition, the skillsets to fulfill those compliance requirements are very hard to come by in today’s competitive market. Another challenge is that a lot of organizations adopt public cloud offerings to increase flexibility, but they lose visibility into the location of their data and they have less control over infrastructure compliance. Data can reside anywhere, even in several different states, each with its own set of data privacy laws. Appropriate data protection controls must be in place for each jurisdiction, which further taxes skillsets, especially if a breach or other issue occurs.

What’s the best strategy to protect data and address compliance?

Knowing the data’s disposition is essential; that means knowing exactly where that data is housed and the type of architecture surrounding it. If the data is on premises, you can implement new technologies as appropriate. Many new tools provide data protection from a backup and access perspective. Organizations should also implement robust data classification policies. Not all data is subject to HIPAA, CJIS, IRS or other regulations. A lot of data is public domain, so it doesn’t need to meet those stringent requirements. Last but not least is applying risk and compliance best practices in accordance with National Institute of Standards and Technology guidance.

Please discuss the growing importance of identity and access management (IAM) technologies in meeting privacy requirements.

Identifying people with the correct level of need-to-know access is critical. HIPAA, CJIS and other regulations clearly document who can access certain data and what they can do with it. Once organizations identify what data needs to be protected, they need a mechanism to ensure people can’t access data they’re not approved to see. Simple authentication technologies such as username/password are no longer capable of preventing unauthorized access. Today’s best practices for protecting sensitive data include mechanisms like multifactor authentication and secure ID tokens, which strengthen identity accuracy.

How can organizations improve the user authentication experience for citizens and employees?

One approach is to utilize standardized directory structures. Having one standardized directory structure eliminates the use of multiple security personas. For example, you don’t need a username/password for transportation services, another for Medicaid and another for unemployment compensation. Besides standardization of directory structures, you can also leverage social media, Department of Motor Vehicles or other large directory structures to validate credentials. The key is using a significant enough directory structure that you don’t have to replicate an identity multiple times. Once you implement multifactor authentication through these mechanisms, you enhance the user experience, as well as the security required for access not only to sensitive data, but users’ own personal data.

What should organizations consider as they contend with the pandemic and “the next normal”?

Organizations should avoid the temptation to skip requirements and get things out there quickly. This crisis forced organizations to establish work-from-home policies overnight. Work-from-home technologies — whether employee-owned or government-issued — must incorporate the organization’s security processes and policies around sensitive data. Government-issued laptops should have remote access capability to keep OS and security product patches up to date, ensure VPN connections are working and generally maintain security standards. It’s also important to conduct and continually reinforce security awareness training focused specifically on working at home or remotely. Then, make the new normal as simple as possible; have everything in place for users to just basically turn on their laptop and log into the system.

With new regulations and new technologies always at the door, how can organizations future-proof their data protection and compliance programs?

It’s important to identify data that doesn’t require a high level of security so you’re not wasting time, effort and money on protecting it. Then, you need to keep abreast of new technology. Vendors like Dell Technologies are at the cutting edge of what’s available to secure and protect data. Leverage those partners and ask a lot of questions, but also do your own homework to understand government requirements from a policy and technology perspective. Identify which data elements are impacted by regulations and need to be protected, and clearly classify that data in your policy. Finally, be realistic. No single solution can magically solve all your problems.
Purpose-built technologies and digital government use cases to take you to the next level

With its end-to-end IT solutions, Dell Technologies help government organizations to:

- Enhance security
- Support workforce transformation
- Modernize and simplify their IT infrastructure
- Deploy new digital services for citizens

Learn more at Carahsoft.com/dell
Simple, Smart and Fast: Search-Driven Analytics for Data Privacy and Compliance

Describe the challenges of identifying, monitoring and protecting data and ensuring compliance in today’s extended enterprise.

As data grows in volume and number of sources, compliance becomes more difficult. The challenge is compounded by the increasing number of citizens and employees who need to utilize that data. Security and compliance must be built into any solution’s DNA from the very beginning. Security has to be at the center of the entire pipeline of data consumption — from how data is collected, to the infrastructure used, to the way it’s analyzed.

How has the pandemic introduced new risks and complexity into data protection and management?

The pandemic further accelerated risk and complexity, especially as more public servants work from home. Today, CIOs and IT workers are essential employees. The work they do is more critical for citizens and the country at large than perhaps ever before. We’re starting to see them use data more and more to deliver these essential services. Addressing issues stemming from the pandemic often requires data from multiple departments and agencies. Bringing all this data together in record time to drive better decision-making while ensuring compliance and protection is no easy feat.

What are search-driven analytics?

Everybody is familiar with search tools. We all know how to go to Google, YouTube or Amazon and enter a few words to search for something. Search-driven analytics brings a similar experience to the world of numbers and data. It allows people to interact with data in a more natural way, with everyday language. Instead of using code, this enables people to interact with data on their own, even if they are not analysts or programmers, and get answers back in seconds. It’s a simple user experience for everyone on the front end, but also provides powerful analytics and infrastructure on the back end.

How can search-driven analytics help alleviate workforce issues such as staffing shortages and lack of trained analysts?

In a recent report by Harvard Business Review, 72 percent of respondents who have brought analytics to their front line workers are seeing significant productivity gains. Search-driven analytics help make that possible because extensive training isn’t required. The easy-to-use language enables anybody in the organization to quickly turn data into insights and actions. Everybody can make better decisions in the moment. There’s no need to rely on data specialists for reports, dashboards or coding for every question. IT workers and analysts can focus on more strategic, higher-level work, such as predictive analytics, data modeling, data curation and data strategy.

What functionality should organizations look for in modern self-service analytics?

One, the technology needs to be simple and intuitive so everyone can use it without extensive training. Two, it must be smart.

Modern analytics must be able to ask questions and also proactively remind users of questions they didn’t know to ask using augmented analytics. Three, for usability, the system must be fast enough to crunch through the insights in seconds. Four, it should be cloud native. With organizations moving more data to the cloud, analytics must be able to find insights for all data living in cloud sources. Last, what makes all this possible is a modern architecture that has the scalability and performance to handle billions of rows of data and look down to the most granular level to extract insights.

Where should organizations start on the road to using business intelligence analytics for data privacy and emerging regulations?

Clearly defined use cases are critical. What questions do agencies need to answer to fulfill their mission, and what data do they need to obtain those answers? Once you find that data, how do you store it, and how do you track compliance requirements on that data? How do you enable data sharing and transparency without interfering with privacy and security? Another critical piece is the criteria and best practices used for tool selection. Can you get to granular levels of data and customize security clearances down to the role level or column level so you can govern who’s seeing what without having to create duplicate data lakes for each department? That can create a list of economies of scale and enable organizations to more easily and confidently share data across agencies.

Learn more at Carah.io/Data-ThoughtSpot

Helen Xing, senior director of global public sector and industry alliances at ThoughtSpot, discusses how agencies can use search-driven analytics to simplify and improve data privacy and compliance.
Advance Your Mission with Insights for Everyone

Make Better Decisions with Search and AI-Driven Analytics for Government Agencies

Learn more at thoughtspot.com/government
Using a Data-Centric Approach to Reduce Risk and Manage Disruption

How can organizations step up their data privacy and compliance programs to weather current and future disruption? Paul Aghabian, global CTO and chief architect for Symantec Enterprise Division of Broadcom, makes the case for a data-centric approach.

How do new privacy regulations and the evolving definition of privacy impact computing and network infrastructure? They have a major impact because key concepts of privacy law — the need for justification to process the data, data minimization, the right to be forgotten and purpose specificity, to name a few — regulate how organizations can collect and process data. Therefore, infrastructures must be able to give them the data they need for their use cases while remaining in compliance with their regulatory obligations. In addition, privacy laws extend to cloud, SaaS-based services and other hosted technologies where the organization’s regulated data may exist.

How has the massive shift to telework and hybrid work scenarios impacted data privacy and compliance?

We see a couple of major shifts and risks. Teleworking has demonstrated the elasticity of traditional perimeter defenses. Now, the enterprise environment needs to extend into the home of every employee who works remotely, and it must protect sensitive data on their machines from attacks and breaches. To do so, the organization has to monitor and collect a massive amount of data flowing in and out of these devices. That data can be used for security but also for other purposes such as performance management or contact tracing. This potentially turns devices into information sources for an employee’s location and offline interactions, leading to mass surveillance risks if the data is ever abused.

Please explain a data-centric approach and how it helps simplify data privacy and regulatory compliance.

A data-centric approach is about being able to understand how data flows and being able to enforce policies and procedures on the data, based on its sensitivity and perceived risk. It’s much more effective to associate policy and controls with a data set that we know contains sensitive data as opposed to applying policies on a particular device. Devices can be an important control point, but the sensitivity and risk is related to the data, and it’s the data that needs to be protected across its life cycle, regardless of where it’s located.

What early steps should agencies take to ensure compliance and manage the costs associated with it?

It’s critical to embed privacy and security considerations early in the design phase of their infrastructure and architecture. Regulatory requirements are constantly changing and they vary by jurisdiction, so you can’t design in a way that’s targeted too closely to any one particular regulatory framework. It’s much easier to manage these things if privacy and security are built in from the beginning and are not an afterthought. Doing so allows for a holistic governance framework and enables organizations to manage risks and costs because they can calibrate compliance and governance to their particular requirements and use cases.

What should agencies watch for as they adopt artificial intelligence and machine learning to streamline data privacy and compliance?

AI and ML have a lot of potential to streamline privacy and compliance, but they also come with certain risks. For example, AI/ML require systems to be trained. If systems are trained inadequately or with inaccurate data, the result may be poor decisions that ultimately cause more damage than good. This is why, as discussions about the use of AI and ML continue, we expect to see more emphasis on accountable development and usage. In practice, this means having requirements around transparency of AI usage, decisions and data quality, as well as robustness in terms of AI security and resilience.

What advice can you give agencies as they modernize and extend their infrastructures to adapt to “the new normal” and future disruptions?

Disruptions are the new normal. They can be cyberattacks, natural disasters, geopolitical tensions, a pandemic like the one we’re experiencing now or the deployment of a disruptive technology like quantum computing. Organizations must expect this new reality and prepare for it by having a consistent governance framework, flexible yet robust cybersecurity and resilience, and a strong understanding of their data flows and data usage. These capabilities enable them to adapt to whatever new disruption may come around the corner.

Learn more at Carahsoft/Data-Broadcom

Delivered with a proven, modernized IT environment.

Welcome to the era of the integrated and agile IT environment. An environment where your government agency is equipped for a future of increased visibility, trusted access to services and more streamlined operations — just the way you operate. It’s an environment where mobile-to-mainframe agility, data access and data protection come together like never before allowing you to balance the needs of implementing new services and updating existing services easily and quickly.

Talk to us about your mission to modernize at www.broadcom.com/ca-software
Leading Through Change

In this Q&A, Jeremy Blaney, senior manager of customer success at Tableau, highlights how organizations can use data to lead through change while self-maintaining privacy and compliance requirements.

What is top of mind for government organizations in terms of data analytics and data management right now?

Leading through the unprecedented amount of change brought by COVID-19 continues to require the use of data and analytics. The first task was to create stability so agencies could keep employees healthy and safe and continue to meet mission and service expectations. Now, as organizations think through re-opening, the new normal is still being defined. Leaders are focusing on what needs to be done to adapt the organization to emerge, grow, and become more digital and data-based. The data imperative underpins all of it—from the early days of the pandemic to where we are now and where we need to go.

How has the massive shift to telework made data management more complex?

A recent statistic said some agencies now have more than 95 percent of their personnel operating in a telework environment. Organizations have faced challenges getting people on private networks because many employees did not have laptops or they lacked the appropriate credentials. Even when employees could access private networks from public domains, additional layers of security prevented them from accessing systems and data stores they routinely use to accomplish their job. Agencies are working through these challenges both for "pre-pandemic" employees and new employees. All of this puts the idea of platform agility and data governance front and center. Many organizations are heading the call, quickly standing up secure and stable environments that can evolve as this new normal continues to define itself.

How can agencies improve data management and governance?

As I mentioned, the first priority of many organizations as they began to lead through the change brought about by COVID-19 was to stabilize. Doing so required not just the use of internal data, but also public data about how and where the virus was spreading. Multiple functional areas—HR, finance, operations—within these organizations needed this data. Pursuing public data in silos isn’t particularly effective. Instead, organizations should be thinking about how they can create single sources of truth through data governance models that support secure widespread access.

What role do automation and machine learning play in managing data and strengthening security and compliance?

Machine learning improves search relevance and ranking so that people use the right data, which certainly benefits compliance. In addition, with relevant data, as identified through a machine learning algorithm, people can get started with their analysis much faster. On the smart analytics front—artificial intelligence, machine learning, statistics, natural language—all of this helps organizations manage their data, because it increases the speed at which they can find high-quality insights or discover unknown unknowns that exist within data. That capability is especially important now as organizations try to map out how to adapt to the new realities of doing government business.

How can organizations help employees make the best use of self-service analytics?

People have been self-servicing analytical needs for years because they need to answer their own questions rapidly. But are people asking the right questions and are they doing all that in the most efficient digital forms? Proficiency is one of the core capabilities defined in the Tableau Blueprint, which is a prescriptive, proven methodology for becoming a more data-driven organization. Proficiency speaks to the need to educate people to see and understand data for decision-making. That includes educating them on how to work with data, measuring the value that they derive from their use of data, and institutionalizing best practices that drive behavior change and informed decision-making.

What kinds of functionality should agencies look for when they select a data management solution?

Data compliance, governance and trust are all woven together in a complex web. In general, data management capabilities need to be governed and self-sufficient so that the solution can respond to an ever-changing data landscape. The solution must provide visibility and control to drive trust in the data environment as a whole. Discoverability—enabling people to quickly and competently find the right data for their analysis—is also important. And last but not least is scale. Data volumes, analytical use cases and data variability are increasing every day. Effectively managing data scale requires repeatable processes that keep data and metadata up to date.

Learn more at Carah.io/Data-Tableau

Leading Through Change
Making sense of a complex world.

Your most important decisions begin with data.

FOR MORE INFORMATION GO TO
tableau.com/leading-through-change
Mark Weatherford has held executive-level cybersecurity positions in both the public and private sectors. He was first deputy undersecretary for cybersecurity at the U.S. Department of Homeland Security from 2011 to 2013. Prior to that, Weatherford was vice president and chief security officer for the North American Electric Reliability Corp., where he directed the organization’s critical infrastructure and cybersecurity program for electric utilities across North America. He also served as chief information security officer for the states of California and Colorado. Perhaps most notably, Weatherford spearheaded some of the nation’s first cybersecurity legislation aimed to protect citizens.

We recently spoke with Weatherford about the future of privacy legislation in the U.S. and the role emerging technologies might play in helping governments contend with growing privacy and regulatory complexity.

The European Union’s GDPR and the California Consumer Privacy Act (CCPA) made big impacts in terms of privacy legislation, and several states currently have their own pending legislation. What do you see happening next? Is a federal law imminent?

The fact that it’s on everyone’s radar is a harbinger that other states will have some form of CCPA at some point. When we first started talking about GDPR, everyone poo-pooed it. Although there are parts of the law I don’t agree with, GDPR made privacy better for the consumer. It raised the bar for how organizations use, collect, share and retain consumer information. The whole life cycle of data has become managed. A couple of years ago that wasn’t the case. CCPA is the first step post-GDPR in the U.S. that’s establishing the course for how we’re going to protect consumer data.

I expect the federal government will take up a privacy law soon. There’s so much personal information out there about every consumer now, and we have to protect it. And I think most security people would agree having a standard federal law or standard federal regulations would make protecting data much easier.

In the wake of this new and pending privacy legislation, how should state and local government leaders change their approach to data privacy?

First, it needs to be a priority. I think most legislators and most state leaders are aware of this issue, but prioritizing it in the stack of other things they’re thinking about and worrying about is a challenge. Second, they need to prioritize it from the perspective of citizens. Despite the best intentions, most organizations are not going to spend money on privacy or security unless there’s a compelling reason to do so. And that compelling reason is typically the threat of fines and legal damages.

What are some critical things state and local government leaders must understand about their data in order to protect it effectively?

Most organizations do not have a good handle on where their data is, who has access to it and how it’s being moved around. Managing risk starts and ends with knowing what data you have and where it lives. Once you know that, you can start implementing controls to protect it. Creating policy is the next big step. Once you have policy in place, that will drive technology and architecture.

Can emerging technologies play a role in helping governments contend with growing privacy rules and regulatory complexity?

Yes, I’m working with several companies that are coming up with innovative ideas around this. One company has developed technology that can tell you where your sensitive data is exactly, which is not as simple as it sounds. There are also several companies that can tell you when people are doing unsafe things with your data, even people who have legitimate privileges and rights to access that data.

How do you see COVID-19 impacting privacy? Will the need for health surveillance blur privacy lines?

Like a lot of things in life, data can be used for good or evil. Our intentions are often good, but mistakes are made. Once we have data, it’s difficult to ensure it’s not going to end up in the hands of bad actors somewhere down the road. I completely understand the rationale for contact tracing around COVID, but we have to protect that data correctly. We need to proceed with caution.
Numerous stories about leadership through the lens of America’s change-makers, including:

HOSTED BY CATHILEA ROBINETT
President, Governing

DOUG BURGUM
Governor, North Dakota

STEVE BENJAMIN
Mayor, Columbia, SC

BLAIR MILO
Career Connections & Talent Secretary, State of Indiana

BETH NIBLOCK
Chief Information Officer, Detroit, MI

CHRIS CABALDON
Mayor, West Sacramento, CA

As automation becomes an ever-more viable tool for government, can policymakers ensure it is used responsibly and ethically?

IN THE BALANCE
While the COVID-19 crisis got most folks thinking about face masks and toilet paper, Chris Calabrese was pondering artificial intelligence and its implications for public policy. His aha moment came when he realized Facebook had sent home most of its human overseers and put AI in charge of policing the social forum for inappropriate content.

“The result has been systems that don’t work as well. They are taking down groups dedicated to sewing masks, just because they are falsely flagged,” said Calabrese, vice president of policy at the Center for Democracy and Technology. “That’s automation being used by one of the most influential companies in the world, and it’s still not up to snuff. That gives me a sense of how far we have to go.”

Facebook’s stuttering steps into automation reflect broader ethical challenges faced by public tech leaders as AI, biometrics and surveillance technologies increasingly enter the mainstream. CIOs are considering everything from the moral implications of came ras on light posts to the ethical fallout from allowing AI to set prisoners’ bail. Will there be bias in AI systems? Will facial recognition erode privacy rights? Around the nation, city-sponsored commissions and academic task forces are trying to tackle some of these tough ethical questions.

“COMPLEX ISSUES”

New York City was an early entrant into the fray. In 2018, local legislation created the Automated Decision Systems (ADS) Task Force to develop policies and procedures aimed at guiding agencies in their use of AI and related technologies.

“The ADS Task Force tackled the complex issues surrounding automated
“THERE IS A TENSION OF HOW GRANULAR AND EFFECTIVE YOU CAN GET WITH THE DATA, WHILE STILL RESPECTING THE BOUNDARIES OF PRIVACY AND SECURITY.”
AI initiative looks at the challenges that stakeholders face in developing, using and regulating this technology. “We are looking at not just the technological side of AI, but at the ways in which these emerging technologies impact everything — from the education of young people, to law and policy, to business, and even issues like democratic engagement and information-sharing online,” said Ryan Budish, assistant director for research.

Researchers here are asking tough questions about AI deployments. How is the system trained? How is it validated? What biases were present in the underlying training data? How can policymakers test the system to be sure it’s not just replicating existing biases?

Budish, too, points to criminal justice as a point of urgent concern. “There are a lot of different organizations out there, some very well intended and some just trying to sell snake oil,” he said. “If you are the IT person in the county court and your administrator wants you to choose a technology to help with this, you might not have the right background to evaluate the different systems. You might not even know the right questions to ask.”

The Berkman Klein Center has looked at a range of state and local issues in which AI could play a part. The technology might be used to detect fraud in welfare benefits, or it could be used to identify which properties should be prioritized for fire-code inspections. Each scenario carries not just practical but moral implications as well.

To assist state and local leaders in their search for answers, the Berkman Klein Center shares best practices. Its researchers have looked at various real-world AI implementation policies, looking for common ground and also highlighting points of divergence. “That helps folks who are trying to think about their own approach to these questions, when they can see what issues other folks are thinking about,” Budish said.

The center also works directly with state attorneys general, helping them to craft policy that responds to the nuanced inner workings of artificial intelligence. “One of the big challenges with AI is that it can be really technical, and then folks just throw up their hands. It seems like magic,” Budish said. “It’s not magic; it is something that people can understand. We can educate folks and put them in touch with experts who can help them to think critically about the way it impacts the work they are doing.”

On the global front, the Berkman Klein Center collaborates with the Organization for Economic Cooperation and Development, and with the International Telecommunications Union, an agency of the United Nations. Through those efforts, the center has helped to develop AI governing principles that have been adopted by 42 countries.

Budish envisions the center as a potential bridge between civic leaders, who may be new to the conversation around the ethics of AI, and academics who have been exploring these issues for years. “There are a lot of places where those conversations are happening, but those conversations are perhaps not always reaching policymakers,” he said.

A NATURAL FIT
Philadelphia began addressing these issues in 2017 with the launch of GovLabPHL, a multi-agency collaboration using studies of human behavior to shape how the city interacts with residents. That effort led to the creation of a road map in early 2019, and those findings in turn are being leveraged today to help guide Philly’s smart city initiatives.
Smart city development is a natural place to put into action the ethical precepts surrounding AI, said Philadelphia Smart Cities Director Emily Yates. All those cameras on light posts, the smart sensors and other apparatuses of civic improvement — these are the front lines of AI implementation.

“We are drilling down into specific topics. What do you attach to a smart street pole? Is AI going to be a surveillance program? And what happens to the data that we are pulling down? We are still fleshing out all of that,” she said.

Yates' office is developing a deep governance structure to ensure that key learnings are incorporated as AI usage increases. This includes executive leadership, an advisory committee, an internal working group and various subcommittees drawn from across city government.

This governmental infrastructure is key to the city's efforts to be responsible in its use of technology. As the big thinkers address weighty questions around ethical usage, “that information has to move up the ladder and across the ladder so that everyone in government is aware of these issues,” Yates said. “It's incumbent on the working group and the subcommittee to communicate to the relevant individuals and also to the mayor’s office, in order to put citywide policies in place.”

Philadelphia Smart Cities Director Emily Yates balances the usefulness of data collected by connected devices with citizen privacy.

In Philadelphia that effort includes deep engagement with the city's data network and security group, whose experts have weighed in on some of the most pressing issues. “There is a tension of how granular and effective you can get with the data, while still respecting the boundaries of privacy and security,” Yates said.

**PRACTICAL VISION**

As cities and states continue to wrangle with the use and potential misuse of new technologies, Yates offers a practical vision. When it comes to the responsible use of data — from automated decisions to biometric-informed surveillance — government will be most successful when it is most transparent.

“If you are going to put up a camera facing a mosque, you need to communicate what you are doing, who has ownership of that data, whether it is public,” she said. “That’s why we have the communications and marketing team as a subgroup working on this. We need to address the community so that they know what we are doing and why we are doing it in a specific way.”

Serious peril looms for cities that fail to address the risks, or that come up with answers but fail to engage the community. Yates points to the big civic projects of the 1960s and '70s that tried to serve a greater good but ended up sowing distrust.

“The worst case is that you spend a significant amount of money, the community gets concerned and then we have to shut it down,” she said. “We don’t want to step backward and deploy technology in a way that makes people worry we might be using it in a way that could harm them.”

Those with a firm grasp of the technological underpinnings as well as community sentiment may be best positioned to help government to state its case as it moves ahead to incorporate emerging innovations.

It's especially helpful to understand the cyclical nature of an AI deployment: The power of this technology lies in the algorithmic ability to learn over time. Civic leaders can take advantage of that to constantly improve upon their uses of the new tools.

“In each stage of that process you need to interrogate your assumptions,” Calabrese said. “Is my data representative of the whole population? Will my assumptions impact everybody fairly? As a government official you can build fairness into the process, and you do that by understanding how this process works.”

"POLICYMAKERS NEED TO BE VERY CONSERVATIVE IN HOW THEY DEPLOY THESE TECHNOLOGIES. IF SOMETHING IS NEW OR EXPERIMENTAL, YOU NEED TO HAVE A LOT OF SKEPTICISM ABOUT HOW IT IS GOING TO DO ITS JOB. YOU CAN’T JUST DEFER TO THE COMPUTER."
Maine lawmakers recently approved a bond package with $15 million to expand broadband in the state, by a lopsided vote of 124 to seven. Gov. Janet Mills then went on to sign the bill the same day, with a provision added to fast-track a statewide vote for the July primary, rather than November as originally scheduled.

The action in Maine is part of a wave of rejuvenated interest in bridging the country’s digital divide, which essentially means making Internet accessible and affordable, as well as equipping residents with technology and the skills they need to use it. And it’s a wave of interest directly owing to the outbreak of the novel coronavirus. Indeed, the Maine vote came right as the COVID-19 pandemic swept the nation, just days after a stark and sudden evening that saw the NBA suspend its season and Tom Hanks publicly announce that he and his wife, Rita Wilson, had tested positive for the virus. Soon after, government leaders the nation over issued mandates for non-essential businesses to close, and health experts stressed the importance of residents sheltering in place to stem the spread of deadly infections. As a result, the nation immediately found itself even more reliant on high-speed Internet than it already was, specifically now on access and connections in homes, not schools, libraries or offices, most of which were closed.

A problem in parts of Maine and throughout the rest of the country, however, is not everyone has access to high-speed Internet, with gaps due to a range of obstacles, including lack of broadband infrastructure, prohibitively high cost or a poor understanding by potential users of how vital the service is to everyday life. Headlines swept the country about school districts trying to hold classes online, struggling because students did not have computers or Internet at home.

In Detroit, for example, only about 15 percent of public school district households have an Internet connection. But it wasn’t just the schools struggling. The nation’s white-collar workforce took to telecommuting, and many soon learned that their home Internet connections were slow, with their neighbors also at homestraining bandwidth.

“What this public health crisis underscores is that broadband is critical infrastructure,” said Kathryn de Wit, manager of Pew Charitable Trusts’ Broadband Research Initiative. “It’s foundational technology to so many things that we in today’s economy rely on every day.”

Amid the homebound social isolation of the coronavirus, society as a whole has never had so stark a reminder of why broadband matters and what life looks like for those who lack access. With that in mind, Government Technology recently spoke with experts, advocates and those working on broadband initiatives in both state and local government. What emerged is a picture of a resurging interest in closing the digital divide, as well as a host of predictions and suggestions around fast-tracking efforts.
most attention to the need for broadband, technology and the skills to use that technology within every American household. Newspapers across the country have documented how school districts and students were unequipped to smoothly transition to e-learning, reporting on lack of high-speed Internet, lack of devices to access that Internet and in some places even a lack of parental understanding about why Internet is important.

The nature of the coronavirus is such that senior citizens are at the highest risk of death. Seniors also inherently have the greatest need to regularly see doctors, a high-risk proposition. Telehealth, however, can enable them to see their doctor without leaving the house. The problem is that seniors are disproportionately on the wrong side of the digital divide.

The other component to all of this is the sudden need for high-speed Internet in residential areas to conduct business as usual at home. What it all adds up to, said Pew Charitable Trusts’ de Wit, is a heightened sense of awareness.

“What’s different right now,” she said, “is these residential options are the only way people can work, or get online to take classes, or interact with their doctors.”

Edmonds, director of digital inclusion for the city of Detroit, has certainly seen an uptick in interest in his work. Detroit became an outbreak hot spot, and with its low rate of Internet in homes, the need is glaring.

Edmonds fielded calls from private-sector companies wanting to donate resources and calls from others asking what he could do with certain amounts of funding. All of this has created a strange and unfamiliar reality for his office, which has never before dealt with an excess of funds nor attention.

It could, however, be a reality that sticks. “Moving on after this, people can’t look away now,” Edmonds said. “We’ve reached a point of understanding that we all have a part to play here.”

The Push for Federal Action

In late January, the U.S. House of Representatives held its first-ever hearing about why Internet is important. Witnesses, including Siefer of the NDIA and Edmonds of Detroit, spoke about their work and issues that would soon become soaringly important.

They also spoke about what they thought should be done to fix this problem, a key part of which is action at the federal level. Another witness was Gigi Sohn, formerly a fellow at the Georgetown Law Institute for Technology Law and Policy.

While others have seen a reinvigoration in interest at lower levels of government, Sohn said it has also recharged the question of whether broadband should be regulated in the same way the government does utilities like phone service.

“Will this reinvigorate the question of whether broadband is a utility?” Sohn said. “It already has.”

Broadband being framed as a utility, of course, is a complex notion, one that deals with the public interest” is liable to be dictated by large private companies.

While the COVID-19 crisis has highlighted the need for people across the country to have reliable Internet, students’ distance learning needs have garnered the most attention for the issue.

In a specific sense, she said this means creating a way for the FCC to hold Internet service providers accountable for how they spend the federal funding they receive. Any action on the part of the FCC, or Congress, seems unlikely to gain traction, given the mix of partisan divide and pandemic response that is currently rolling almost the entire federal government.

There is, perhaps, some reason to be optimistic, and it can be found at the level of state and local government, where a recent report by Pew Charitable Trusts has found growing momentum for connectivity efforts. In January and February, reports from overseas began to suggest that the United States should prepare for the onset of the novel coronavirus. Almost simultaneously, Pew Charitable Trusts released a report noting that state government work to boost broadband accessibility and availability had, in recent years, gained momentum.

At the time, it was difficult to draw a link between the two, but that has since changed.

The report was the result of 18 months of research on all 50 states, specifically homing in on 10 state case studies. But when the pandemic confined millions to their homes soon after, scores of state governments have already put much work into bridging the connectivity divide, primarily by working to foster better broadband access.

The push for broadband as a utility has been ongoing for years. In 1996, President Clinton signed the Telecommunications Act, a major telecommunications bill that for the first time recognized broadband as a utility. While others have seen a reinvigoration in interest at lower levels of government, broadband being framed as a utility has rarely been a priority for decision-makers in both the public and private sectors, several state governments have already put much work into bridging the connectivity divide, primarily by working to foster better broadband access.

But as digital equity work becomes a new priority for decision-makers in both the public and private sectors, several state governments have already put much work into bridging the connectivity divide, primarily by working to foster better broadband access.

ThePushforFederalAction

In late January, the U.S. House of Representatives held its first-ever hearing on digital equity. Witnesses, including Siefer of the NDIA and Edmonds of Detroit, spoke about their work and issues that would soon become soaringly important. They also spoke about what they thought should be done to fix this problem, a key part of which is action at the federal level. Another witness was Gigi Sohn, formerly a senior staffer at the Federal Communications Commission (FCC) and presently a fellow at the Georgetown Law Institute for Technology Law and Policy.

While others have seen a reinvigoration in interest at lower levels of government, Sohn said it has also recharged the question of whether broadband should be regulated in the same way the government does utilities like phone service.

“Will this reinvigorate the question of whether broadband is a utility?” Sohn said. “It already has.”

Broadband being framed as a utility, of course, is a complex notion, one that deals with the public interest. Sohn said it has also recharged the question of whether broadband should be regulated in the same way the government does utilities like phone service.

“In a specific sense, she said this means creating a way for the FCC to hold Internet service providers accountable for how they spend the federal funding they receive. Any action on the part of the FCC, or Congress, seems unlikely to gain traction, given the mix of partisan divide and pandemic response that is currently rolling almost the entire federal government.

There is, perhaps, some reason to be optimistic, and it can be found at the level of state and local government, where a recent report by Pew Charitable Trusts has found growing momentum for connectivity efforts. In January and February, reports from overseas began to suggest that the United States should prepare for the onset of the novel coronavirus. Almost simultaneously, Pew Charitable Trusts released a report noting that state government work to boost broadband accessibility and availability had, in recent years, gained momentum.

At the time, it was difficult to draw a link between the two, but that has since changed. The report was the result of 18 months of research on all 50 states, specifically homing in on 10 state case studies. But when the pandemic confined millions to their homes soon after, scores of state governments have already put much work into bridging the connectivity divide, primarily by working to foster better broadband access.

But as digital equity work becomes a new priority for decision-makers in both the public and private sectors, several state governments have already put much work into bridging the connectivity divide, primarily by working to foster better broadband access.
During a recent conversation with Government Technology, de Wit pointed to an overarching lesson: There's no magic bullet — no incentive, regulation, law or partnership — that by itself can fix the digital divide. A vital lesson made clear by the 10 case studies is that the most effective approach is several different actions working toward the same goal.

With that in mind, there are two states that rank as perhaps the best example of what government can accomplish: Maine and North Carolina.

A ‘Germination Seed’ for Broadband in Maine

First and perhaps foremost, Maine and North Carolina are both part of an increasing number of states that have created dedicated offices and full-time staff positions to work on broadband availability and accessibility, as well as other digital inclusion efforts.

And while their work tends to deviate in its execution from there, the general approach that each takes is familiar — the goal is to find solutions to the broadband challenge that are specific for each individual community in the state.

Indeed, in separate conversations with officials in both states, each used the old saying, “If you’ve seen one county, you’ve seen one county,” meaning that what works in one part of the state will almost certainly not work in the exact same way in another.

Maine has a program called ConnectME that was founded in 2006, powered primarily by a small fee related to landlines and some broadband connections. The initiative has a budget of roughly $1 million, an oversight board, and a small staff, led by Executive Director Peggy Schafer.

One of the most impactful approaches that ConnectME takes involves fostering community engagement among influential community members. Planting this “germination seed,” as Schafer described it, is often an easy first step.

“When you have no Internet or you have really bad Internet,” Schafer said, “it’s not really that hard to get the community engaged with how to improve it.”

One lesson that Schafer and others have learned in Maine is that this buy-in is not entirely about business or economics, and that it also requires getting communities to understand how Internet can help seniors see their doctors, encourage young adults to stay in their communi-
ties, and help children do their home-
work — lessons all made more acute by the onset of the COVID-19 pandemic.

That’s all well and good, but where Schafer often sees the biggest chal-
lenge is when there’s a financial need. A community will reach a consensus that broadband is vital, and often they’ll create specific plans for how to build out infrastructure, perhaps centered around a public-private partnership specific to their region. They still need the money to make it reality, either via government grants or the invest-
ment of a would-be private partner.

Schafer was heartened to see money allo-
ated to broadband support efforts in some of the recent federal government stimulus efforts, although she said she’s hopeful it will be a start to more investments.

“When you pull pots of money together, you can get significant projects done,” she said.

And she’s certainly heard from more people at all levels of governments wanting to get digital inclusion projects done, adding that “this emergency stripped the cover off of this issue.”

The North Carolina Broadband Playbook

North Carolina has taken a similar approach to the issue, doing so through its Broadband Infrastructure Office. Jeff Sural has been the director of that initiative since early 2015.

In the government broadband and digital inclusion space, many experts and advocates point to North Carolina as a state government success story, noting that it takes a largely singular approach to the work by having a team of people on the ground state-
wide. Sural describes this group — officially named the Technical Assistance Team — as the state’s geek squad. Really, the group sounds like a broadband mission impossible squad, with each member having different expertise, ranging from Wi-Fi technicali-

ties to economic development concerns.

Over the years, the team has repeatedly found that every county is unique. Even so, they’ve identified a pattern of shared challenges and concerns, which led to the creation of the Broadband Community Playbook. Its first suggestion is for the area to form its own Broadband Community Planning Taskforce, made up of local people from all different areas of communities — school districts, private industry, economic development and more.

The driving idea is that the communi-
ties will do the work of creating a means of broadband availability that works for them, with the state team serving as something like technical advisers. To this end, their playbook also offers up checklists, RFPs and example ordi-
nances related to placing wireless equip-
ment on public assets like water towers.

“We tried to lead up with tools and checklist and things like that to make it more tangible so these folks can do the work themselves,” Sural said of the playbook.

His office is also engaged with building tests and surveys aimed at giving the state a comprehensive and uniform data set related to broadband, something that has long proven elusive throughout the United States, with frequent criticisms over the FCC’s broadband mapping.

“The end result is that there are rural areas of North Carolina where 90 percent of households are connected to high-speed fiber Internet, which is a rate higher than in many major cities. Sural attributed this to the years of work the state has invested, the skill sets of the members on his team, the patience of small Internet service providers to wait for return on investment and the willingness of local entities like electric co-ops to help with infrastructure.

While his counterparts are fielding waves of calls from parties surprised at the extent of the digital divide, Sural said that in his state the importance of the work has long been recognized. There’s just a renewed push nationwide to get the work done.

“I’ve been hearing from my colleagues around the country,” Sural said, “and right now, everyone is just working overtime to try and come up with ways to solve this.”

srapairman@geovitech.com
While the first few months of 2020 were notable to be sure, they were perhaps especially daunting for the new permanent state chief information officers who stepped up to their posts amid the turmoil of the novel coronavirus. But the business of government IT pressed on, and while these CIOs were tasked with challenges like quickly transitioning to telework, shoring up cybersecurity and tracking COVID-19 data, the nuts and bolts of gov tech remained: modernizing legacy systems, expanding broadband and coordinating with state leadership on long-term priorities.

Our editorial staff got to know this new class of state CIOs, checking in as they settled into their positions at an unprecedented moment in history.
TRACY BARNES
INDIANA

Transparency is a cornerstone of the leadership style Tracy Barnes brings to his position as the head of Indiana’s Office of Technology (IOT). He prefers to engage fully with staff at all levels of the organization, sharing what he knows and relying upon their expertise to make the best possible decisions. But he started the job at the end of March, the same month the state saw its first case of COVID-19. That reality has made the kind of communication he seeks a little harder.

“I want to figure out how I make sure I get that message out there in a comprehensive manner to the full footprint of the agency so everyone understands the value that they’re bringing, especially in this time where tensions are high, pressure is high and expectations are high,” he said. “The ability to walk up and down the aisles and just say ‘hi’ or ‘good job’ or ‘attaboy’ are limited and probably won’t be available at any true capacity for a while.”

Barnes brings a multi-faceted background to the CIO job, having worked extensively in the ERP area in private industry and higher education both in the United States and abroad. He made the move to government a few years ago as IT director for the state auditor’s office, then as chief of staff for the lieutenant governor. As state CIO, Barnes acknowledges the strong foundation built through the expertise of his predecessors and looks forward to bringing his enterprise-level skills to bear in order to move all agencies forward using technology.

A proponent of as-a-service technologies, Barnes envisions that establishing a sustainable, supportable multi-cloud offering will be a critical part of meeting the state’s needs. He wants to solidify IOT’s role in guiding agencies toward secure solutions that fit within the broader operational IT framework, especially in areas like data integration. Noting that technology investments tend to outlive the agency leadership that was in place at the time of the purchase, he takes a longer-term view of IOT’s responsibility.

“We need to make sure that folks still at the state can continue supporting them and managing them and maintaining them for potential turnover and for succession planning down the road,” he said.

ANNETTE DUNN
IOWA

Annette Dunn is no stranger to the inner workings of government. She was named by Gov. Kim Reynolds to the CIO role in July of 2019, following a four-year stint as IT division director and CIO of the state Department of Transportation. And her DOT post came on the heels of nearly a decade in other roles with the state — notably among those as a key player in a statewide project to equip snowplows with GPS and advanced vehicle location technology that has since been used in a number of other states.

Taking on the state CIO job comes with similar challenges as roles she’s previously held, Dunn said, just on a bigger scale. And rising costs and flat or declining budgets place even more pressure on IT resources.

“We must provide the innovation and access to Iowans that they expect and need,” she said. “This puts a larger burden on the use of data and technology to help us make more strategic decisions and think outside of the box to be able to deliver services in more convenient and customer-friendly ways.”

Getting a handle on the state’s data is a major priority for Dunn. She’s eyeing a robust data warehouse that can be relied upon as a resource to users across the state in order to inform the best possible business decisions. And there’s work to be done to get there: getting a clear picture of the data held by various state systems; deduplication and standardization; and establishing access controls.

“The creation of a strong, reliable data warehouse that is easily utilized will make us a stronger state and help us make better business decisions now and well into the future,” she added.

Her approach to leading the broader IT organization is to look both outward and inward. She sees vendor partners as playing a critical role in helping agencies meet their technology needs, as they can move more quickly and efficiently, often at a lower cost. But pivoting away from internal development is a big cultural shift, which explains why internal communication is another huge area of focus.
“From a leadership standpoint, it comes down to changing the culture and helping people see the big picture,” she explained. “I spend a lot of time convincing employees that change is just a different way of doing things, and at the end of the day there will always be work for them to do that is important and necessary.”

JEFF WANN
MISSOURI

Jeff Wann was on the job two weeks when the coronavirus spreaded in Missouri, and across the country, all but shutting down the state.

“And everything changed,” Wann remarked on the last day of April, as the state counted more than 7,500 confirmed cases of COVID-19, and 329 fatalities related to the disease. Missouri Gov. Mike Parson declared a state of emergency on March 13.

Earlier this year, Wann was named Missouri’s new CIO, bringing a long career spanning the public, private and nonprofit sectors. He was tapped, in part, for his leadership in the job of modernizing Missouri’s Office of Administrative IT Services.

An overarching goal was “to help modernize the IT systems, and to help transform processes and procedures, and to help further mature the IT organization,” said Wann.

“The COVID-19 situation has helped us to accelerate that,” he said. “It’s a silver lining in a very dark cloud, because obviously, COVID-19 is a terrible thing for folks. But on the other hand, it’s been a catalyst to help us to be able to help our citizens. And frankly, help other states.”

The crisis required quick action in a number of areas. Tools like chatbots, which can take months to develop, were being turned out in only weeks and days. The state teamed up with the Missouri Hospital Association to launch a new tool, developed by Google, to form a marketplace that matches state suppliers of personal protective equipment with health-care workers. Telephone, GIS and other systems were upgraded and improved to meet the new challenges the crisis called for.

When Missouri does return to more normal operations, Wann plans to return to his punch list for modernizing IT.

“Now, it’s going to be tough,” he added. “Because projected revenue in fiscal year ‘21 is not looking good for any state.”

“But I expect to keep going,” Wann continued. “I expect that now that we are training our people in these new technologies, we can continue on doing those things with the budgets as they are.”

BROM STIBITZ
MICHIGAN

When he started as Michigan CIO on March 4, Brom Stibitz was prepared.

A lifelong resident of the state, besides still being in college, Stibitz had been chief deputy director of the Michigan Department of Technology, Management and Budget for five years. Before that he had been director of executive operations for the state Department of Treasury, a senior policy adviser, and a legislative director at the state House of Representatives.

He was ready to hit the ground running.

Then the pandemic hit.

Like most state CIOs, Stibitz had to set aside what he thought he’d be doing this spring and instead manage organization-wide emergency measures, including telework on a scale that Michigan had never attempted before. He spent much of those first weeks overseeing preparations for nearly 28,000 state employees: doubling VPN firewall capacity, finding laptops and organizing staff training on various tools for working from home.

He defines his broader priorities for Michigan as efficient and effective government, IT accountability, customer experience, and (of course) cybersecurity. He said those weren’t explicit directives from Gov. Gretchen Whitmer, but they appeared to be shared goals among state departments.

“There’s been a lot of focus on, how do we make sure that services of the state are accessible to people, not just that it’s there and people can use it, but how do you make it so people can understand it and it’s truly accessible?” he said.

“The other area of focus has been efficiency. How do we make sure that we’re consolidating around solutions instead of expanding the state’s footprint?”

Asked what recent IT projects he’s most glad to have done, Stibitz mentioned a couple that weren’t flashy, but critical: developing a single sign-on solution, now used by more than 200 applications, to simplify security; and transitioning state employees to Microsoft Office 365, which reduced their reliance on network storage, revealed several practical and budgetary efficiencies, and unwittingly prepared the state to work from home.

In April, Stibitz was fairly sanguine about the results of the state’s telework operation, but under no illusions about the economic challenges to come.

“We’re looking at precipitous declines in revenue over the next six, 12, 18 months,” he said. “So there’s going to be more pressure than ever on IT to (a) find efficiencies within what we’re doing, and (b) find solutions that can help agencies or customers save money.”
JOHN SALAZAR
NEW MEXICO

When John Salazar became New Mexico's IT secretary on March 2, he knew he'd have to address issues such as dated infrastructure and broadband access. What he didn't know was that his new role would soon revolve around responding to a pandemic that would infect more than 1 million Americans within two months. The workload has been gigantic.

"We're working weekends. We're working nights. It's been a challenge for us," Salazar said.

The first big hurdle was ensuring that roughly 20,000 government employees could work from home. Salazar thinks the mission was accomplished, but not without hiccups. The state filed an emergency order with a vendor for 1,000 laptops, but the machines came a month late, so Salazar's team had to get creative in an IT structure where agencies manage their own networks and workstations.

"The first couple of weeks were chaos," Salazar recalled. "We were all working in different directions."

He spent a lot of time in April collaborating with the New Mexico Department of Health, which has two legacy systems that receive COVID-19 testing data from the Centers for Disease Control and Prevention. The goal was to create a dashboard with relevant information for Gov. Michelle Lujan Grisham, which required Salazar's team to, among other steps, stand up a platform in the cloud and develop data interfaces between the legacy systems.

Having previously worked as a CIO in two different state agencies—Taxation and Revenue, and the Department of Workforce Solutions—Salazar was well prepared for his position as head of New Mexico IT. But no one could foresee the long-term impact of COVID-19. Salazar attempted to compare the situation to Y2K, but he pointed out that at least with Y2K, there was a "long climbing process" during which people knew what was potentially coming.

Now leaders like Salazar must react in ways that might forever change how states utilize technology. He sees plenty of opportunities to improve New Mexico's systems by incorporating more cloud solutions, automating more processes and putting in place more procedures for better cybersecurity.

As for government meetings, New Mexico is holding a tremendous amount of virtual sessions—a new trend that perhaps should be a norm.

"All of our employees are doing this on a regular basis, and that's something that probably needs to continue in the future," Salazar said.

TRACY DOAKS
NORTH CAROLINA

Tracy Doaks is a self-proclaimed technologist at heart. "I love talking about it, translating that in business terms so that I can talk about it with different audiences, understanding the finance side of it," she said.

That was essential in her last four years as deputy CIO in North Carolina, where she primarily focused on back-of-house operations like data centers, the state network, and cloud and identity management. Since she took the head post as CIO in March, Doaks has had to pivot to more outward-facing work, coordinating with the governor's office and doing more public speaking. "Now my focus has expanded to all facets of the Department of Information Technology [DIT]," she explained, "so that includes cybersecurity, data analytics, rural broadband, 911, digital transformation."

Doaks has spent 20 years in and out of government, in the North Carolina Department of Revenue, where she was CIO, as well as time in health care and with Accenture. That experience meant she primarily focused on back-of-house operations like data centers, the state network, and cloud and identity management. Since she took the head post as CIO in March, Doaks has had to pivot to more outward-facing work, coordinating with the governor's office and doing more public speaking. "Now my focus has expanded to all facets of the Department of Information Technology [DIT]," she explained, "so that includes cybersecurity, data analytics, rural broadband, 911, digital transformation."

Doaks has spent 20 years in and out of government, in the North Carolina Department of Revenue, where she was CIO, as well as time in health care and with Accenture. That experience meant she primarily focused on back-of-house operations like data centers, the state network, and cloud and identity management. Since she took the head post as CIO in March, Doaks has had to pivot to more outward-facing work, coordinating with the governor's office and doing more public speaking. "Now my focus has expanded to all facets of the Department of Information Technology [DIT]," she explained, "so that includes cybersecurity, data analytics, rural broadband, 911, digital transformation."

Some of those challenges included putting together a coronavirus website in just a few days to help pull heavy Internet traffic away from Health and Human Services, as well as supporting similar issues at the Division of Employment Security.

And the pandemic of course heightened the need to expand broadband connectivity, particularly throughout the state's rural areas, which Doaks had to quickly get up to speed on. "As the schoolchildren and college kids were sent home and employees were sent home," she said, "that made it even more critical and a top priority for us."

JERRY MOORE
OKLAHOMA

Jerry Moore took the reins as Oklahoma’s new CIO in February, at a time when the state’s IT organization and direction was shifting. Gov. Kevin Stitt, who appointed Moore, has made it known he is pursuing a new direction for Oklahoma IT, prioritizing digital transformation and modernization as two of the main efforts of his administration.

Part of this has involved a reorganization of the state’s Office of Management and Enterprise Services: OMES is in the process
of conducting an audit meant to identify unnecessary expenditures, which was ongoing when Moore came on the scene. Having spent a decade as the CIO for the Tulsa Technology Center — the educational IT hub affiliated with the Oklahoma Department of Career and Technology Education — Moore is no outsider to government work. Before becoming CIO, he also worked as the state’s director of IT application services.

At the same time, it is his private-sector experience that has likely given Moore the skill set that is most appealing in light of the governor’s effort: Having held IT leadership roles for large companies like ConocoPhillips and SiteTraxx, Moore has consistently shown an ability to take on IT restructuring projects that hew to long-term strategic goals.

Stitt has said this is what he hopes Moore will bring to the job: the ability to deliver high-performance, cost-effective solutions as the state navigates its modernization efforts.

“Jerry’s more than 20 years of experience in technology leadership in the public and private sectors will serve Oklahomans well as we continue our efforts in becoming a top ten state,” said OMES Director Stephen Harpe in a statement. “He has a proven record in identifying and executing new technologies to solve business problems.”

LUCAS ROPEK

JEFFREY CLINES SOUTH DAKOTA

A drive to help people, rather than increase margins and decrease bottom lines, is what brought Jeffrey Clines to public-sector work. He began his career in the private sector, then spent more than a decade in operations and enterprise applications for the American Heart Association. But even that nonprofit work didn’t fully yet at Clines’ desire to impact real people’s lives. In 2018 he moved to government, as CIO for the Illinois Secretary of State’s office, before becoming head of the South Dakota Bureau of Information and Telecommunications this past April.

“I believe that in technology, you can’t stay in one place,” Clines wrote in an email to Government Technology. “We push forward, finding ways to leverage technology — especially emerging tech — to improve service, systems and processes.”

He’s committed to working with state agencies to target where they want to go and see how tech will help get them there.

“There is no stable ground anymore,” he said. “The days of being able to stand up a system and have it work for 20 plus years are no longer here.”

That forward-looking approach to state IT has so far served him well during his tenure, which of course began amid the COVID-19 pandemic as South Dakota moved to nearly all remote work. When Clines thinks about when the U.S. will “return to normal,” he hopes it doesn’t.

“If we push to go back to where we were, we may lose some of the valuable lessons we have learned in this process — things like the ability of our teams to work independently and remotely, or how we have really pushed to look at ways to be creative in delivering services while maintaining social distancing.”

One area where Clines sees this having the most impact is on rural communities as people are given the option to work away from city centers and be just as productive. South Dakota is home to many scenic, far-flung areas that Clines hopes to reinvigorate via telework, which he notes will need investment in broadband and other critical infrastructure to thrive.

LAUREN HARRISON

BILL SMITH ALASKA

Bill Smith took up the role of Alaska’s state CIO in late 2019, a turbulent time for the state IT department. He became the fifth person to hold the job since 2018, after a series of interim leaders.

Why the turnover? The state had launched an effort to centralize its technology offerings, and the process “didn’t go as well as everybody wanted,” Smith said. The job nonetheless appealed to him because, as he saw it, the fundamentals had begun to fall into place.

“The state leadership is very supportive, from the governor to all the cabinet-level department leaders. We’ve also brought in external resources, where before the centralization effort was being done entirely in-house,” he said. “I believe the conditions exist now for us to have long-term success with this effort.”

Those external resources included a third-party assessment of the overall IT ecosystem, which Smith is now leveraging as the basis for prioritization. He also is busy updating all the technology-position descriptions to align with a modernized IT environment, and he’s taking a fresh look at the service catalog.

“We want to build out the organizational chart more fully, to nail down what the services are, how we will provide those and with what resources,” he said. This will include an overhaul of IT governance, with an eye toward creating a more collaborative relationship between the Office of Information Technology and state agencies.

“I’d also like to be able to be the broker,” he said. “If the departments have an IT need, my team can figure out what services are available, so that the departments can focus on meeting their own business needs.”

ADAM STONE

J.R. SLOAN ARIZONA

J.R. Sloan joined Arizona state government in 2013 as manager of the digital government program. He moved to the
DeAngela Burns-Wallace was already heading up the cabinet-level Department of Administration in Kansas when the governor tapped her to take on an added role as leader of the independent Office of Information Technology Services (OITS).

In her new position, which she’s held since August 2019, Burns-Wallace has staked out a number of key goals. She’s looking to modernize legacy systems and putting a heavy emphasis on security. “Our security posture is solid, but I want us to not just be ‘in the moment,’” she said. “I want us to be in a more strategic stance, strengthening our overall security posture not just as individual agencies but in a coordinated way across state government.”

Data governance also is high on her agenda. “We have some data sharing that has come together out of necessity, but now we need to take a step back and put a real strategy and structure around that,” she said. “We need to put in place sustainable guidelines and policies that aren’t susceptible to changing leadership or changing political winds.”

Finally, Burns-Wallace said she is looking to elevate the perception of IT as a dependable partner across all levels of state government. “We have to have reliable, consistent high-quality IT services across all of our agencies. But over the years, that consistency and level of quality have been uneven,” she said. “Non-cabinet agencies for instance have not always gotten the same level of service, and yet their work is incredibly important. They have a significant impact for our state.”

Going forward, Burns-Wallace said OITS needs to establish a more level playing field, in order to change perceptions at the agency level. “There needs to be a reliably high level of service across all those entities,” she said. “That’s how we rebuild trust and confidence in what IT is delivering.”

RUTH DAY
KENTUCKY

Ruth Day took the helm at Kentucky’s Commonwealth Office of Technology (COT) in December 2019 amid a flurry of bad news.

Two months earlier, a state auditor faulted COT’s inventory practice, saying the agency couldn’t account for some $765,000 worth of equipment. Then in November, a contract worker with access to COT’s storage rooms was indicted for allegedly stealing more than $1 million in laptops from the agency.

Despite the potentially fragile environment, Day rose to the challenge of helping state agencies respond to the COVID-19 outbreak just a few months after taking on her new role. In mid-March she issued a memo to guide officials in their use of online meeting platforms. When vulnerabilities appeared in the popular Zoom platform, she quickly followed up with further guidance.

Meanwhile, Day continues to lead COT in its efforts to address a number of key issues. Supported by COT, state offices have begun to connect to KentuckyWired, a state-run project constructing high-speed fiber-optic infrastructure to every Kentucky county. Looking ahead, COT will be supporting the National Guard in mounting Cyber Protection Teams to secure the upcoming primary and general elections.

Prior to her appointment, Day served as the vice president for administrative services at Landstar System Inc., a transportation services company specializing in logistics. In a press conference at the time of her appointment, Day expressed enthusiasm for the work ahead. “I’m honored to join the [Gov. Andy] Beshear-[Lt. Gov. Jacqueline] Coleman administration and I think you can tell that the [governor] has laid out a very clear and concise mission for me...,” she said. “I’m very excited and ready to go to work for Kentucky.”

DEANGELA BURNS-WALLACE
KANSAS

DeAngela Burns-Wallace was already heading up the cabinet-level Department of Administration in Kansas when the governor tapped her to take on an added role as leader of the independent Office of Information Technology Services (OITS).
What’s Your Emergency?

Texting rather than calling 911 in an emergency has become increasingly viable, but parts of the country still lack the option. Here’s a look at how far the tech has come.

BY BEN MILLER, ASSOCIATE EDITOR
A man who was high on heroin and wanted by police came to his sister’s day-care center. A group of deaf people became stranded in the middle of a large lake when their boat’s motor died. A woman was kidnapped by a trucker at a rest stop, sexually assaulted and then left in the back of his cab as he drove. These are all real stories, and in each situation the people involved either couldn’t call 911 or would have put themselves in jeopardy by doing so.

So instead, they texted. The police came to take the woman’s brother into custody, bring the boaters back to shore, and arrest the truck driver and rescue his victim. These stories — just three of countless examples that happen every day — prove why it’s important for 911 dispatchers to have the technology that allows them to receive texts instead of just phone calls. And in point of fact, the Americans with Disabilities Act mandates that emergency services provide equal access to people who can’t speak or are hard of hearing.

But many — maybe most — dispatch centers in the U.S., called public safety answering points (PSAPs), are not yet capable of taking text messages. They’ve made a lot of progress in the past several years, but Zainab Alkebsi, policy counsel for the National Association of the Deaf, said it’s not nearly common enough.

“Imagine being in the middle of an emergency and being unable to contact 911,” she wrote in an email to Government Technology. “That is what deaf and hard-of-hearing people experience when faced with an emergency.”

If one takes the number of PSAPs each state reports as being text-capable to the federal government each year and adds them up, then divides by the total number of PSAPs, the data suggests that 34 percent of them were text-capable in 2018, the most recent year of data. However, for reasons discussed here, the total PSAP count is not a highly reliable figure.

THE SHAPE OF PROGRESS

To be clear: All available evidence suggests that text-to-911 has become more available to more people in more places in recent years.

Data from the National Highway Traffic Safety Administration’s annual National 911 Progress Report shows that the number of texts sent to emergency dispatchers each year rose from about 1,000 in 2014 to more than 188,000 in 2018. And it’s not because of a growth in the number of 911 contacts, either — texts made up 0.001 percent of all 911 calls in 2014; by 2018 they were 0.09 percent of all 911 calls.

It should be noted that emergency dispatchers prefer that people call if they’re able to and if doing so wouldn’t put them in danger. Calls often provide a more accurate location to the dispatcher and can also convey other important information such as background noise.

The portion of PSAPs capable of receiving texts — an undercount,
to be sure — grew from 5 percent in 2014 to 14 percent in 2018.

Since emergency communications are handled on a state-by-state basis — and often on a county-by-county basis — there are big geographic disparities to text-to-911 as well.

That’s clear when looking at available data for both the number of texts sent to 911 and the estimated percentage of PSAPs that are text-capable in each state, as shown in the maps accompanying this article. As of 2018, at least five states appear to have achieved coverage over their entire area: Connecticut, Delaware, Massachusetts, Vermont and Minnesota. Another 12 have surpassed 50 percent.

That means 34 states are either below 50 percent or lacked sufficient data to be measured.

The problem is that it’s hard to show a comprehensive, detailed picture of which locations have the option available and which don’t. The information that is available tends to be patchwork and lags a year or two.

**SHADOWY FIGURES**

It’s actually very difficult to tell how widely available text-to-911 is, or even to show all the places where it is available. The FCC and NHTSA have made efforts to do so, but their information is largely self-reported by states and individual PSAPs, so much data for individual states and years is missing.

There are also some discrepancies in the data, and since it’s mostly gathered by survey, it’s entirely likely that there are more that aren’t readily apparent. And because the data isn’t very detailed, it’s not easy to show where in each state text-to-911 is available, or to get a good sense of how many people have access to the option.

Even with complete information, the metrics presented here have their limitations. The percentage of PSAPs that are text-capable, for example, definitely underrepresents the actual availability of the technology.

**THE MINNESOTA APPROACH**

The state of Minnesota is a perfect example of why PSAP counts don’t tell the whole story. Despite the fact that only 34 of the state’s 97 primary PSAPs are capable of receiving text messages, anyone can text 911 anywhere in the state.

**TEXTS TO 911 IN 2018**

While five states report complete text-to-911 coverage, nearly two-thirds are either below 50 percent coverage or coverage cannot be measured with available data.

**Total Texts Sent to 911 in the U.S., 2014-2018**

<table>
<thead>
<tr>
<th>Year</th>
<th>Texts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>1,121 texts</td>
</tr>
<tr>
<td>2015</td>
<td>34,700 texts</td>
</tr>
<tr>
<td>2016</td>
<td>102,163 texts</td>
</tr>
<tr>
<td>2017</td>
<td><em>No data available</em></td>
</tr>
<tr>
<td>2018</td>
<td>188,646 texts</td>
</tr>
</tbody>
</table>

*No data available for 2017.*
state of Minnesota and be sure that it will reach an emergency dispatcher.

Minnesota took a regional approach to implementing the technology. In most places, regional dispatch centers will receive a text and then route it to the appropriate local PSAP.

That was a very deliberate approach, according to Emergency Communication Networks Division Director Dana Wahlberg.

“One of the decisions we made as a state before we implemented was we wanted an ubiquitous rollout, we didn’t want it to be sporadic,” Wahlberg said.

“We have 301 PSAPs in the state. We didn’t want 10 or 12 of them to roll it out and then have the public be confused about whether they could use the service.”

In addition to rolling it out everywhere at once when the systems went live at the end of 2017, the state also had unified operational and technical standards and one big public awareness campaign to let people know about the new option.

Other states have followed that approach, Wahlberg said. But that’s not how all states have done it — and indeed, in some states the regional strategy would be much more difficult to accomplish.

THE TEXAS OPTION

Take Texas, for example. Where Minnesota has strong central governance over its PSAPs, Texas has three different governing bodies that all handle different groups of PSAPs — one that mostly handles county dispatchers, one that handles city dispatchers and one for the state’s wide swaths of rural areas.

According to Kelli Merriweather, executive director of the Texas Commission on State Emergency Communications (CSEC), her state likes to give PSAPs a little more local control over how they do things. And as it happens, federal data shows that Texas was one of the first states anywhere in the country to have text-to-911 available. But at first it tended to be in urban centers with larger populations.

The smaller, more rural areas, which fall under the jurisdiction of the regional planning commissions, were another beast. Working with the regional commissions, Merriweather and the CSEC coordinated to come up with specifications so that they could give each area a guide for what they needed, while taking care to avoid creating a need for a lot of expensive new equipment. Some needed software patches, some needed new equipment. There was a lot of working with small, regional telecommunications firms.

But between 2017 and the end of 2019, every regional planning commission became text-ready. And now Texas, which was the first state with a significant level of text-to-911 availability, is among the few states with wide geographic availability of the service.

“It’s hard with such a vast area like that and all the diversity of equipment in the PSAPs out there;” she said. “It takes a long time to turn the ship.”

THE INDIANA METHOD

Indiana is another state that jumped onto text-to-911 early, but has relied on individual areas to adopt it on their own. Ed Reuter, executive director of the Indiana Statewide 911 Board, said the technology has spread as early adopters have demonstrated success and shared best practices.

“There were initial concerns that this was going to cause more work for the dispatchers … they might have to hire more people,” Reuter said. “Well, it’s really proved otherwise, because the generation of telecommunicators that has been brought in over the last few years, this is all they’ve really known.”

One of the practices that has spread across Indiana is texting citizens back when they call 911 and the call is dropped. That method, which Reuter said came from his time at the PSAP in Bartholomew County in the southeastern part of the state, has become so popular that most Indiana PSAPs send far more texts than they receive.

“When that call comes in, instead of calling them back — and it could be that they could be in a dangerous situation or unable to talk — dispatch would send them a message,” he said.

A CLOUD OF UNCERTAINTY

It’s hard to know exactly how widespread text-to-911 is. But what’s even less knowable is the number of times, every day, all across the country, that people who can’t speak, people who are hard of hearing and people who are in dangerous situations are unable to reach an emergency dispatcher because their local systems can’t take texts. All we know is that the number is far larger than zero.

That could have very real life-and-death consequences for many people. But it also means the removal of some people from civic institutions. Wahlberg, the emergency communications director in Minnesota, told a story of a time when a woman in her state who was hard of hearing and non-verbal came across a car in a ditch. She texted 911 to alert the authorities, and the situation was resolved. Her texts with the local dispatchers included a little more, too pride.

“Because text was available, she felt she was able to help a fellow citizen,” Wahlberg said.

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>0.05%</td>
</tr>
<tr>
<td>2015</td>
<td>0.09%</td>
</tr>
<tr>
<td>2016</td>
<td>0.13%</td>
</tr>
<tr>
<td>2017</td>
<td>0.22%</td>
</tr>
<tr>
<td>2018</td>
<td>0.34%</td>
</tr>
</tbody>
</table>

*Source: Federal Communications Commission, National Highway Traffic Safety Administration*
Privacy and the Law

Some states seek to emulate California’s sweeping though yet-to-be-enforced digital privacy legislation, while action stalls on the federal level.

By Pamela Martineau

As Americans spend more time hopping from Zoom meetings to retail websites to news sites — especially during increased time at home due to the coronavirus — some are increasingly concerned about protecting their digital privacy and data. Lawmakers throughout the nation are responding by working to pass online privacy legislation on the state and federal levels. But controversy over who should enforce the laws, the definition of consumer information, and whether citizens should be able to sue companies in the event of a data breach or other violation are among the top issues holding up legislative efforts. And with lawmakers focused on pressing coronavirus impacts, legislative efforts on digital privacy are largely paused, experts say.

“There are a lot of proposals in many state legislatures,” said Hayley Tsukayama of the Electronic Frontier Foundation. “But with the coronavirus, many have reassessed their priorities about what’s moving and what’s not … and many [proposals] are not.”

Still, legislative movement is expected when the nation returns to some level of normalcy, and when it does, California will likely retain its reputation as a leader in the quest for online privacy with its California Consumer Privacy Act (CCPA), which went into effect on Jan. 1, 2020. Some states view it as a template for their own measures.

“California is definitely a standout in a lot of different ways … it has set the standard and the bar that other states are following,” said Ashley Johnson, of the Internet Technology and Innovation Foundation (ITIF). The Golden State’s efforts have spurred action — or at least discussion — of the issue at the federal level. But whether a bipartisan compromise can be achieved remains to be seen.

Here’s a look at what some digital privacy experts view as standouts in legislative online privacy efforts at the state level, and some of the sticking points in those and federal proposals.

Federal Proposals

Two key bills are pending in the Senate Committee on Commerce, Science and Transportation — one from Committee Chairman Roger Wicker, R-Miss., and another from ranking member Maria Cantwell, D-Wash. The bills contain some similar provisions to California’s and some overlap, but differ in key areas. Wicker’s bill would override any state measure, and Cantwell’s would not. Cantwell’s also contains the controversial private right of action provision, which has been the sticking point in some state legislation. Wicker’s contains no such provision.

Johnson believes it is important that a federal bill override state measures so “every company in the U.S. knows what to expect,” rather than have to adapt to 50 different sets of rules. Her organization also does not support private right of action provisions. She said the CCPA’s provisions granting private right of action in limited circumstances has kept proponents of the provision from compromising on the federal level in that regard.

“They have gotten their way in California,” she said, adding that her organization would rather see a federal law where
breaches. In addition, EFF is concerned for every privacy violation, not just data. Johnson also believes the act “disincentivizes” data collection needed for emerging technologies such as artificial intelligence and the Internet of Things (IoT). “We think it might stymie innovation in AI and IoT,” she said.

Tsukayama, of EFF, said one of her organization’s concerns about the CCPA is it only allows private right of action lawsuits in limited circumstances involving data breaches. Her organization has proposed follow-up legislation allowing people to sue companies for every privacy violation, not just data breaches. In addition, EFF is concerned that the CCPA does not have strong enough enforcement provisions. Under the act, the state attorney general would bring suit in cases of violation. Tsukayama said the AG’s office has stated it can only handle two to three such cases per year. “We run the risk of having these really grand-sounding pieces of legislation that sound like they do a lot, but when the rubber hits the road, there’s not enough resources there to make sure consumers get the protections that are in the laws,” said Tsukayama.

Daniel Castro of ITIF (and a Government Technology columnist) said he supports the CCPA’s provision of “notice to cure,” where a company, if given notice of a violation, would then be advised to amend the violation within a set period of time. “In a way, that idea can potentially mitigate a lot of concerns about lawsuits,” said Castro.

Castro said other states are looking to implement similar notice to cure provisions in their legislation. California has recently enacted other privacy laws, including measures that require the AG’s office to make information from data brokers available on its website and a law pertaining to smart televisions that prohibits the recording of voices through voice recognition software.

Other States
Maine and Nevada have recently passed privacy laws that are fairly comprehensive, according to Johnson. “These efforts aren’t just concentrated where you would expect the most technologically aware states — like our Californias, New Yorks or your Washingtons,” said Johnson. “All states are looking at it.”

Online privacy legislation is also pending in Illinois, Wisconsin, Massachusetts, Minnesota, Pennsylvania and New Jersey. Measures in Washington and New York failed — largely over private right of action provisions.

Johnson said the New York measure introduced a controversial legal concept of information fiduciary, which introduced a legal standard of care regarding collected personal data. “It was something a lot of people could not get behind,” she said.

Tsukayama said she believes the coronavirus crisis will change the tenor of the online privacy debate, drawing more people into the debate, since more people are online now, giving the passage of bills a greater sense of immediacy. “We are spending so much time online now, and using all of these tools that have not been used this much before the crisis,” she said, with people using Slack for book clubs, Zoom for family reunions or office conferences, and other online tools. “I actually think that privacy protections are more important than ever.”
Austin Names New Security Chief
Veteran cybersecurity professional Shirley Erp started work as CISO of Austin, Texas, at the beginning of June. Her previous roles include cybersecurity director and adviser at KPMG, as well as CISO for the Texas Health and Human Services Commission and assistant CISO of the University of Texas system, among other private- and public-sector work.

Data Officer Appointed in Los Angeles
Jeanne Holm, most recently senior technology adviser to Los Angeles Mayor Eric Garcetti, was named the city’s new chief data officer. Holm has also held the roles of deputy CIO and assistant general manager of L.A.’s Information Technology Agency. She replaces Lilian Coral, who served as the city’s first CDO since 2016.

Wisconsin CIO Steps Down
After eight years at the head of Wisconsin IT, David Cagigal announced his departure in June. Cagigal, a 2020 Government Technology Top 25 Doer, Dreamer and Driver, served under both Republican Gov. Scott Walker and Democratic Gov. Tony Evers. His time with Wisconsin included accomplishments like developing cybersecurity guidelines to assist local governments, and initiatives like BadgerNet, which provides broadband for state offices, schools and libraries throughout Wisconsin. As of press time, a replacement had not been named.

California Selects Digital Innovation Director
After a year-long search, Gov. Gavin Newsom selected Udaya Patnaik as the first director of the California Office of Digital Innovation (ODI), part of the state’s Government Operations Agency. ODI’s mission is to work “collaboratively with state agencies to improve digital services for Californians,” including prototyping new ideas and advising on existing projects. Patnaik founded Bay Area-based tech firm Jump Associates in 1998, where he served as senior partner and chief financial officer.

California Highway Patrol IT Chief Retires
Scott Howland, CIO of the California Highway Patrol, retired in June. Howland, a recipient of Government Technology’s Top 25 Doers, Dreamers and Drivers award for 2018, was head of the agency’s Information Management Division for six years, capping a 30-year career in law enforcement. He was replaced by Christopher Childs, a CHP officer who most recently was assistant chief in the Enforcement and Planning Division.

California Selects Digital Innovation Director
After a year-long search, Gov. Gavin Newsom selected Udaya Patnaik as the first director of the California Office of Digital Innovation (ODI), part of the state’s Government Operations Agency. ODI’s mission is to work “collaboratively with state agencies to improve digital services for Californians,” including prototyping new ideas and advising on existing projects. Patnaik founded Bay Area-based tech firm Jump Associates in 1998, where he served as senior partner and chief financial officer.

California Highway Patrol IT Chief Retires
Scott Howland, CIO of the California Highway Patrol, retired in June. Howland, a recipient of Government Technology’s Top 25 Doers, Dreamers and Drivers award for 2018, was head of the agency’s Information Management Division for six years, capping a 30-year career in law enforcement. He was replaced by Christopher Childs, a CHP officer who most recently was assistant chief in the Enforcement and Planning Division.
News & Insights on Where Government Is Going

GOVERNING
THE FUTURE OF STATES AND LOCALITIES

Get Our Free Daily Newsletter: governing.com/newsletters
Virtual View

Lenovo announced the Lenovo Mirage VR S3 headset with the ThinkReality application platform. The all-in-one headset was developed in conjunction with Pico Interactive, a technology company that builds VR and enterprise software. The headset features a 4K display for clearer visuals, hands-free control for use with or without the provided controller, and an easily cleaned hygienic face plate suitable for mass use. Built with integrated audio and up to three hours of battery life, the Mirage VR S3 is rugged, lightweight and specifically designed to scale within the enterprise. www.lenovo.com

Small but Mighty

The Dell Precision 3240 Compact Workstation is an ultra-small form factor workstation designed for tight workspaces and edge computing. This small but powerful system can operate with up to seven displays and is virtual-reality-ready, with an optional NVIDIA Quadro RTX 3000 graphics card. The device comes with a 10th Generation Intel Core-i9 or Xeon processor up to 8 cores, up to 64 GB of RAM and up to 4 GB of storage. The workstation has several mounting options; and dust and wire covers, giving it more flexibility in device placement. www.dell.com

Virtual View

Lenovo announced the Lenovo Mirage VR S3 headset with the ThinkReality application platform. The all-in-one headset was developed in conjunction with Pico Interactive, a technology company that builds VR and enterprise software. The headset features a 4K display for clearer visuals, hands-free control for use with or without the provided controller, and an easily cleaned hygienic face plate suitable for mass use. Built with integrated audio and up to three hours of battery life, the Mirage VR S3 is rugged, lightweight and specifically designed to scale within the enterprise. www.lenovo.com

On the Go

The new FUJITSU LIFEBOOK U7310 notebook incorporates a 10th generation Intel Core processor, along with a 13.3-inch screen, light weight from 1.17 kg and a Thunderbolt 3 connector, for mobility and portability. The 19.2 mm notebook also offers a high-definition or full-high-definition (FHD) display, anti-glare, FHD touch panel option, magnesium housing, and optional backlit keyboard. The U7310 contains up to 40 GB of memory and battery life of almost 14 hours. The webcam’s privacy camera shutter prevents unauthorized hacking and access. Security is supported with the optional integrated PalmSecure palm vein sensor or fingerprint sensor. www.fujitsu.com

For more product news, log on to explore Government Technology’s Product Source. govtech.com/products
DOWNLOAD TODAY: GOVTECH.COM/LIBRARY

WHEN HINDSIGHT IS 2020
WHAT HAVE WE LEARNED 20 YEARS AFTER Y2K AND WHERE ARE WE GOING NOW?

ANNUAL THOUGHT LEADERSHIP PAPER BY THE CENTER FOR DIGITAL GOVERNMENT

© 2020 e.Republic. All rights reserved.

GT20 AD Annual TLP.indd 6/3/20 4:49 PM
100 Blue Ravine Road
Folsom, CA 95630
916.932.1300
www.erepublic.com
Forging Ahead

As we navigate toward an unknown new normal, gov tech leaders continue to find innovative ways to lead.

These unprecedented times offer little in the way of a playbook for IT teams and their colleagues. In the face of the COVID-19 crisis, state and local government technology shops moved mountains to accelerate remote working — in many cases in a matter of a few days. As the fallout from the pandemic continues, public-sector IT will be called upon to demonstrate thought leadership across the organization.

One silver lining is robust: Accessible digital services are no longer considered a nice-to-have or a bonus. Stubborn staff members, typically in non-IT departments, now realize that digital signatures, electronic procurement processes and mobile payments are not only feasible but also offer numerous benefits for citizens and staff alike. Suddenly, IT initiatives once thought impossible by some became possible overnight.

As Microsoft CEO Satya Nadella half-joked, “We’ve seen two years’ worth of digital transformation in two months.” The challenge of “shadow IT” poses a more significant threat now than ever. Various teams needed to move quickly to survive in March and April, and, in some cases, did so without direct IT oversight. Relationship building, communication and collaboration are often more important for CEOs than the standard Microsoft versus Google decisions. The long-predicted CIO-as-a-service-broker vision continues to gain steam as a likely model moving forward.

In this way, IT can help other departments consolidate and renegotiate contracts and agreements. CIOs and IT directors are typically highly skilled at contract and agreement negotiations. This moment presents an excellent opportunity to lend those talents to non-IT discussions. While many of our colleagues often avoid these difficult conversations, we can help them engage in collaborative but candid negotiations with vendors and partners. Smart, strategic and cost-effective agreements must be the norm for government agencies.

IT will also play a crucial role in the months ahead if government organizations are going to do more with less staff. Visionary leadership will realize that if agencies need to continue operations with fewer full-time employees, tech will play a central role in maintaining and enhancing services. The old IT-as-a-cost-center concept will undoubtedly rise this year, but technology demands are not declining. Needs and threats are soaring, and new opportunities are here as well. If done correctly, we can save money and increase efficiency.

Smart city solutions will now face greater scrutiny and vetting — as they should. Smart city projects that don’t offer tangible benefits to the vast majority of our residents and constituents won’t pass muster. Projects that don’t provide a quick return on investment should face skeptical review. If nothing else, COVID-19 has proven over and over that resilience conquers all. Shiny smart city projects that don’t truly move the needle will lose their luster this year. It didn’t seem possible, but cybersecurity is now even more critical. Remote workers, cloud application sprawl and bad actors looking to exploit this crisis have created even more landmines for IT to navigate. The Center for Internet Security offers numerous resources and road maps for hardening our defenses. Now is also the time for state and local leaders to consider a version of the Cybersecurity Maturity Model Certification (CMMC) created by the Department of Defense for their vendors. We are only as strong as our vendors’ cybersecurity postures, and we need a mechanism to ensure they are doing their part.

This moment presents an excellent opportunity to lend those talents to non-IT discussions. While many of our colleagues often avoid these difficult conversations, we can help them engage in collaborative but candid negotiations with vendors and partners. Smart, strategic and cost-effective agreements must be the norm for government agencies.

IT will also play a crucial role in the months ahead if government organizations are going to do more with less staff. Visionary leadership will realize that if agencies need to continue operations with fewer full-time employees, tech will play a central role in maintaining and enhancing services. The old IT-as-a-cost-center concept will undoubtedly rise this year, but technology demands are not declining. Needs and threats are soaring, and new opportunities are here as well. If done correctly, we can save money and increase efficiency.

Smart city solutions will now face greater scrutiny and vetting — as they should. Smart city projects that don’t offer tangible benefits to the vast majority of our residents and constituents won’t pass muster. Projects that don’t provide
48% of Americans surveyed in early 2020 by industry organization Partners for Automated Vehicle Education said they would never get into a self-driving taxi. Twenty percent said they think the tech will never be safe. However, only 8 percent of those surveyed were familiar with the accident in Tempe, Ariz., where an autonomous Uber struck and killed a pedestrian, so many fears of AVs seem to be of undefined origin.

**NIGHT SHIFT:**
Following an announcement from the Metropolitan Transportation Authority in early May that the New York City subway would be shut down between 1 a.m. and 5 a.m. every night for coronavirus-related cleaning, the agency worked with a Swiss company called Axon Vibe (not to be confused with body-camera manufacturer Axon) to quickly roll out an app to help essential workers navigate the city in those early morning hours. Called Essential Connector, the app points users to nearby available buses; if none are available, one free taxi ride is offered per night. The system is designed to become more personalized over time as it learns a user’s frequently visited stops.

**$5.5M:**
Following the widely reported 2017 Equifax breach that revealed sensitive personal and financial data of 147 million Americans, the credit monitoring service agreed to pay each affected individual $125 as part of a settlement with the Federal Trade Commission. While that amount isn’t likely to make it into Americans’ bank accounts any time soon — $125 multiplied by nearly 150 million proved too much for Equifax to pay — the company has agreed to provide $5.5 million to “all financial institutions in the United States” to cover the costs of reissuing any compromised credit cards.

**Disinfecting Drones**
When large gatherings and events are being held once again, new hygiene measures will likely be in place for cleaning spaces like sports stadiums. Buffalo, NY-based startup EagleHawk proposes drones equipped with disinfecting sprayers as the solution to ensure stadiums are safe post-event, while cutting down on cleaning time compared to wiping down everything by hand, as well as limiting worker exposure to the virus. EagleHawk plans to offer its service to sports teams in its home region.

Send Spectrum ideas to Managing Editor Lauren Harrison, lharrison@govtech.com
Throughout the early months of the COVID-19 pandemic, we’ve seen new leaders emerge at all levels of government. It is fascinating to watch the good, the bad and the ugly regarding public speaking with so much at stake. But while this pandemic is new, preparing to answer difficult questions in hard times is a skill we can learn.

Technology and security leaders can be confronted with loaded questions that appear to offer no easy way out. Whether the query is coming from staff, management, customers or even the press, how can we prepare and offer workable answers for those inevitable “gotcha” traps that come our way?

For example, consider questions like, “Are you 100 percent sure that every staff member is healthy and frequently tested, and that no one will spread COVID-19 to your customers?” Or, “What mission-essential technology projects have been canceled due to new pandemic-related priorities?” Or, “Can you guarantee no data breaches occurred when staff transitioned from working in the office to home and back to the office?”

No doubt, there are often common traits to flag potential danger ahead regarding these verbal land mines. Watch out for: all-or-nothing caveats in questions (such as “no data breaches,” or that “every person” will “always” be tested); loaded words that, when combined, set you up for failure (like “mission-essential” and “canceled”); and someone asking for promises to be made about things that are outside of your control.

**Trick Questions Are Not New**

More than a decade ago, I attended a leadership seminar in Michigan that taught us how to be aware of, and how to respond to, hostile news media questions. This helpful class encouraged us to practice answering the question that the person “should have asked,” if they were being polite. That is, regard the question in your mind and answer the question positively. Word of warning. Never repeat the negative question in your verbal answer.

For example, if a reporter asks, “Why are you wasting taxpayer money?” don’t reply defensively by saying, “I’m not wasting taxpayer money!” The message the audience will receive is that you probably are wasting taxpayer money, regardless of what you say next. Instead, answer a more positive version of the reporter’s question. “I am responsibly spending every precious tax dollar that our government receives by implementing using best practices from respected organizations like the National Institute of Standards and Technology.”

Include the team involved and describe the process being followed. Even if you don’t have an exact answer to a question, be prepared to walk through the steps your team is taking to implement best practices.

**Three Tips for Answering Tough Questions**

So, what else can help?

First, build confidence by preparing for these situations. Just as we prepare for security incidents and system outages with tabletop exercises, security and technology leaders need to take time to practice our communication skills with colleagues.

While working with public information officers and other communications staff is essential in communicating effectively to your internal and external audiences, don’t assume that help will always be available to address tough questions. Rather, build a culture where leaders are prepared to know the best-practice answers to all types of questions, and to deliver the message in the right tone and context. Work on delivering approved talking points with supportive stories if time permits.

Second, use appropriate humor when possible. No one was better at this than President Ronald Reagan. When asked a challenging question about prayer in schools being illegal, he reportedly said, “As long as there are final exams, there will always be prayer in the schools.”

Third, describe the process being followed. Even if you don’t have an exact answer to a question, be prepared to walk through the steps your team is implementing using best practices from respected organizations like the National Institute of Standards and Technology. Include the team involved and describe how they are contributing to reaching agreed-upon goals with a unified playbook.

Remember, in a job interview, the best-prepared candidate, and not always the most talented person, often gets selected for the position. Do your homework, and don’t get caught in the trap of thinking that no one will ask tough questions once you get the job.

**Daniel J. Lohrmann**

Daniel J. Lohrmann is the chief security officer and chief strategist at Security Technology and is an internationally recognized cybersecurity leader, and author. From 2002 to 2014, Lohrmann led Michigan’s award-winning cybersecurity programs, serving as CSO, CTO and CISO.
FEELING DISCONNECTED?

CONNECT WITH YOUR PEERS
(and get smarter!)

Check out our live webinar schedule.

govtech.com/webinars
Stop the care and feeding of your servers

Seamlessly manage everything from finance to enterprise asset management with cloud-hosted government software from CentralSquare. Get up and running instantly and scale as your community grows, with no upgrade costs or downtime.

Schedule a demo today at centralsquare.com.