THE PUSH AND PULL OF PRIVACY

HOW TO MOVE GOVERNMENT FORWARD WITHOUT LEAVING CITIZENS BEHIND.

INSIDE:

Facing Biometrics
The possibilities and dangers of facial recognition.

Privacy for Business
Approaches and advice for gov tech companies.

PLUS:

Who’s in Charge?
Data on where chief privacy officers sit in states.
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
COVER STORY

14 / Practical Privacy
As concerns about protecting online personal information grow and little is done at the federal level, states — and their IT leaders — take bold steps.
By Adam Stone

35 / Facing the Future
Thanks to massive gains in accuracy and lower costs, facial recognition is better than ever. But is the technology a threat to our privacy?
By Tod Newcombe

40 / The Price of Doing Business
Many tech companies that sell to government agencies are working to minimize the personal data their products collect. Why? Because citizens demand it.
By Zack Quaintance
DEPARTMENT

10 / States Tackle Privacy
A look at the rise of the chief privacy officer.

COLUMNS

6 Point of View
Opting in to privacy.

8 Data Points
What can we learn from GDPR?

9 Four Questions
Maryland CIO Michael Leahy on his priorities for the state and what lies ahead.

46 Cybersecurity Strategies
Are you ready for 2020?

50 GovGirl on Social
The importance of staying relevant.

NEWS

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

47 Spectrum
More research, more science, more technology.

48 CIO Central
Career change across tech-driven roles in government.

IN OUR NEXT ISSUE:

Gov Tech Blasts Off
Space: the next frontier for government?

Census 2020
The trade of local IT shops in making sure everyone is counted.

Advancing Agile
Training “lean coaches” to drive efficiency.
2019 DIGITAL GoVernMenT SuMMIT

Spreading Best Practices & Spurring Innovation

ATTEND/SPONSOR:

govtech.com/events

JOIN US

Alabama
Arizona
Arkansas
California
Chicago
Colorado
Connecticut
Florida
Georgia
Illinois
Indiana
Kentucky
Los Angeles
Louisiana
Maine
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
Nevada
New Jersey
New York
North Carolina
Ohio
Oklahoma
Oregon
Pennsylvania
Tennessee
Texas
Utah
Virginia (COVITS)
Washington
Wisconsin
Opting In to Privacy

The title of the current federal privacy law is the Privacy Act of 1974. That’s right, 1974, when a stamp cost a dime and a gallon of gas cost about 50 cents. Despite its age, many of its central tenets hold up rather well.

The act set out to govern how federal agencies could use the personally identifiable information they held, requiring permission from the owner of the data in order for it to be shared with another agency. While exceptions were plentiful (e.g., statistical uses like the Census, routine government business, congressional investigations, law enforcement, etc.), the intention was to protect citizen privacy from government overreach. People also have the right under the law to review information held about them by federal agencies.

There have been a couple of updates to those broad policies over the years that took into account database matching programs (1988) and added exemptions for the Department of Homeland Security (2007) related to travel. An executive order in 2017 eliminated Privacy Act protections for non-citizens.

What’s absent from these updates, however, is sweeping federal policy that acknowledges the added vulnerabilities unearthed in recent years by the data practices of private-sector players that trade in personal information on a massive scale. In light of the European Union’s General Data Protection Regulation (GDPR), companies operating in the U.S. feverishly updated their privacy policies to clarify their business practices to consumers. But it’s still the job of the individual to opt out. There’s a growing belief that this burden is misplaced, and that it should rest with the service provider who should have to secure an opt-in to data sharing from users of their services.

While we wait for the feds to act with some updated national rules, many states have stepped in with their own privacy solutions. According to legislative tracking website Quorum, more than 200 pieces of legislation on privacy have been debated in state legislatures so far this year alone.

I’ve written before in this column about the California Consumer Privacy Act, which empowers consumers with additional rights relative to the collection and use of their personal data. Gov. Gavin Newsom has further proposed a “Data Dividend” that would put a price on an individual consumer’s data and potentially allow them to profit from it.

Meanwhile in Maine, as we were preparing to publish this issue of the magazine, Gov. Janet Mills signed what was being called the strictest privacy law in the United States. The bill requires Internet service providers to get permission from consumers before they sell their personal information. The bill also says ISPs can’t make the sale of data a mandatory part of their service terms, nor can they punish those who opt out by charging them more or by any other means. While it only pertains to ISPs (for now), Maine has charted new territory with the country’s first “opt-in” bill.

Our cover story, Practical Privacy (p. 14), includes an interview with the author of Washington state’s much-debated attempt at a privacy law in its most recent legislative session. Ongoing back-and-forth with tech giants resulted in a bill that was ultimately stymied by privacy advocates who felt its protections didn’t go far enough. While stopping short of Maine’s “opt-in” approach, the bill by state Sen. Reuven Carlyle would have allowed consumers to know what data was being gathered and whether it was being sold. Further, consumers under the bill could correct inaccuracies, delete their information altogether and opt not to have their information sold.

Carlyle has vowed to try again in the next session. He won’t be the only one. We’ll continue to follow legislative efforts across the country, as well as when the issue makes sufficient headway to lead to a new federal privacy policy reflective of the Internet economy.

“From the standpoint of efficiency, it would be much easier to have a federal law that gave everyone exactly the same standards and the same road map for dealing with data and data protection,” said Maryland Secretary of Information Technology Michael Leach (read his interview in Four Questions, p. 9). “But I think it’s a bit early to move in that direction.”

It promises to be a bumpy few years.
Street Smarts
Santa Clara County, Calif., is using edge computing to improve traffic flow on its congested 10-lane arterial roads, sending real-time data from sensors and video cameras that calibrate signal times for some 1.5 million cars each day to the county’s Traffic Management Center. Other sensors detect when a bicycle approaches an intersection or the speed at which a pedestrian is crossing a street, allowing them sufficient time to cross safely.

GOING OFF THE SHELF
In May, Gov. Tim Walz decided to scrap the state’s troubled Minnesota Vehicle Licensing and Registration System (MNLARS) and asked CIO Tarek Tames, along with other stakeholders, to procure a software package instead. The system was first under contract with Hewlett-Packard, until the state opted to build it in-house. Its 2017 rollout was plagued by high downtime, a lack of consumer support and incorrect fee charges.

Biz Beat
A three-step process from cloud computing company Rackspace aims to help smaller software-as-a-service vendors become compliant with FedRAMP, the Federal Risk and Authorization Management Program. FedRAMP Authorization to Operate is often a prohibitively high standard for small companies, and Rackspace’s program could make the gov tech market more accessible to thousands of software providers.

WHO SAYS?
“As you know, with paper-based processes, things move slow. Well, 911 and slow don’t mix well.”

MOST READ STORIES ONLINE:
For Second Time in a Year, Baltimore Hit with Ransomware
Seattle Tech Chief Dismisses 14 Directors, Middle Managers
Major Reorganization of Florida IT Agencies Imminent
Handful of States Begin Legislating “Deepfake” Videos
Arizona Shifts from Disparate Email to Google’s G Suite
Micro-Mobility Is Here to Stay — Cities Should Act Accordingly

The amount the Knight Foundation is contributing toward fostering Miami’s startup ecosystem.

The number of public safety agency customers CentralSquare is giving its Aware software to for free, hoping to reduce emergency response times nationwide.

The age of Wyoming’s Revenue Information System, which state officials estimate will take $68 million and 10 years of staff training to replace.

The percentage of Americans likely to buy an electric vehicle as their next car purchase, according to a AAA survey.

The amount the Knight Foundation is contributing toward fostering Miami’s startup ecosystem.

The number of public safety agency customers CentralSquare is giving its Aware software to for free, hoping to reduce emergency response times nationwide.

The age of Wyoming’s Revenue Information System, which state officials estimate will take $68 million and 10 years of staff training to replace.

The percentage of Americans likely to buy an electric vehicle as their next car purchase, according to a AAA survey.

The amount the Knight Foundation is contributing toward fostering Miami’s startup ecosystem.

The number of public safety agency customers CentralSquare is giving its Aware software to for free, hoping to reduce emergency response times nationwide.

The age of Wyoming’s Revenue Information System, which state officials estimate will take $68 million and 10 years of staff training to replace.

The percentage of Americans likely to buy an electric vehicle as their next car purchase, according to a AAA survey.
What Can We Learn from GDPR?

Five lessons the U.S. can take from the European Union’s privacy regulation efforts.

On May 25, 2018, a new data privacy law went into effect in the European Union. This law — the General Data Protection Regulation (GDPR) — has been held up as a global standard for consumer data protection. It has also created momentum for lawmakers in the United States to introduce their own proposals for regulating data privacy. Yet one year later, consumers, businesses and regulators are all dealing with a variety of unintended consequences. Given that GDPR has fallen short of expectations, policymakers in other countries have an opportunity to do better, rather than repeat Europe’s mistakes.

Harmonize Rules

One of the primary rationales for GDPR was to create “one continent, one law” so that companies could more easily do business in Europe. Yet in trying to copy the EU, many U.S. states are considering, or have already passed, their own privacy laws, which would create a fragmented market in the United States. Notably, some countries in the EU are still not compliant with GDPR. The U.S. should pursue a single federal data protection law to avoid re-creating these issues.

Avoid Hurting Internet Users

European consumers were worse off by many metrics after GDPR went into effect. Not only were consumers inundated with online cookie notifications, new corporate privacy policies and requests to re-join email lists, but they were also cut off from some websites. For example, one analysis found that more than 1,000 U.S. news sites blocked access in the EU to avoid compliance challenges. And to add insult to injury, according to a survey in March from the European Commission, nearly two-thirds of Europeans (63 percent) do not know exactly what GDPR is — not surprising given that the law is over 250 pages long. U.S. policymakers should remember that data protection laws have significant impact across businesses, large and small, in every sector, and should aim to create simple rules that consumers can understand.

Don’t Constrain Innovation

GDPR makes it too difficult for businesses to collect and use data, particularly by requiring organizations to specify how they will use data at the outset and minimizing what they collect. This means that they cannot collect data without knowing specifically how it will be used and they cannot reuse data for novel purposes. In addition, GDPR limits automated decision-making by requiring companies to provide human review of significant decisions and information on the logic involved in those decisions. Combined, these restrictions make it particularly difficult for EU companies to use artificial intelligence. As the United States is attempting to remain a leader in AI, it should not create a regulatory environment that unnecessarily hampers its ambitions.

Minimize Compliance Costs

Implementing GDPR has been an expensive undertaking. The 300 largest global companies have so far spent more than $7 billion on initial compliance. For example, GDPR requires companies to appoint a data protection officer. Yet a recent survey found that for a majority of companies (52 percent), this position serves no valuable business function and instead is only for compliance. U.S. data protection efforts should avoid rules that force companies to focus on check-the-box compliance and instead encourage them to concentrate on investing in areas of their business that could meaningfully reduce the risk of consumer harm.

Avoid Regulatory Overload

GDPR sets a high bar for reporting data breaches, with organizations obligated to report incidents within 72 hours of discovery. This tight timeline, coupled with fears about severe fines for non-compliance, has resulted in organizations over-reporting in an effort to be transparent. The multinational law firm DLA Piper has noted that “regulators are stretched and have a large backlog of notified breaches in their inboxes.”

Given the problems with GDPR, the United States should avoid repeating these mistakes and instead strive to create a national privacy framework that streamlines regulation, pre-empts state laws, establishes basic consumer data rights and minimizes the impact on innovation.
Maryland Secretary of Information Technology Michael Leahy has been head of the state's IT department since March 2017, first in an acting capacity and then permanently. In that time, he has established strong foundations for efficiency and interoperability across the enterprise. After consolidating agency IT and standardizing data governance and management, Leahy is now looking ahead to how to fine-tune the organization for both employees and the public.

**1. What is your approach to securing the state?**

Our principle concern goes to the questions that you have to answer by not knowing what you don't know, so we're looking at implementing tools on an enterprise basis that will give us a better picture of how folks are operating within the network and also finding ways to make sure our employees are more aware of the cyberconcerns out there. Fully half of the problems that people have with incidents and breaches are because their employees either succumb to a phishing attack or pick up a device and plug it into a USB port. A big piece of our concern goes to making certain the state workforce is aware of cyberhygiene and then making full use of the tools that we've brought in to protect our network.

**2. What challenges are you seeing around workforce?**

We have a number of open positions, and because we're in the D.C. area, it's both a blessing and a curse. There is an immense amount of talent, but we have a hard time competing with the private sector and other parts of the state, federal and local governments in paying what those folks pay. A more fun challenge is there are lots of opportunities to make a difference and make our workforce and our work more customer-centric and citizen-centric.

**3. How are you addressing growing privacy concerns?**

The largest issue we're going to have is the question of “Who owns the data?” I personally am sympathetic to the European model that data about a subject is the property of that subject. You get into all the arguments about it really property, or just an attribute. If it's just an attribute, there can't be questions of ownership, so I think the attempts underway in California and New Jersey are going to be the first to deal with these issues in the United States. I'd like to see us deal with that issue in a way that gives people more control of their data and how they interact with the government based on that data.

I'm a big believer in the experimentation of democracy, and having 50 models gives one the opportunity to innovate and address very real questions that people don't think about until they become an issue for them. It would be much easier to have a federal law that gave everyone exactly the same standards and the road map for dealing with data and data protection. But I think it's a bit early to move in that direction.

**4. What's the outlook for 5G in Maryland?**

When anyone asks me about 5G, I ask them what they mean by 5G. There are so many different definitions and avenues for possibility. But here in the state, we're looking at using 5G principally to move data faster without worrying so much about backhaul. That's going to open opportunities for smart cities and for things being more available to the public simply because we have a faster path to get there. There are some advantages to 5G that will come to the forefront for serving rural populations, but we're a few years away from that becoming mainstream because the principle efficiencies can be found in urbanized areas.

— Lauren Harrison, Managing Editor
As technology gets more sophisticated, it collects more and more data. And government has a better ability to store it. And cybersecurity attacks keep exposing people’s personal information.

So it’s no surprise that more states are now hiring chief privacy officers (CPOs). As highlighted in a 2019 report from the National Association of State Chief Information Officers, there were only a few state CPOs up until the last couple years, and most are the first to hold their position in their state.

GovTech decided to dig a little further into the role, who holds it and how they operate. In conducting our own search, we found 11 states that had CPOs, though the titles varied from place to place. They are Arizona, Arkansas, Indiana, Kentucky, New Jersey, Ohio, South Carolina, Tennessee, Utah, Washington and West Virginia.

Their work often revolves around managing legal risk, ensuring compliance with privacy doctrines like HIPAA and creating standards around data privacy as governments collect more data and share it between agencies more often.

In two of those states — Arizona and Washington — the position is currently filled by an interim or acting CPO. Additionally, information wasn’t available for all CPOs on all questions.
TWO STATE CPOs AREN’T IN IT DEPARTMENTS:

INDIANA: Indiana’s CPO, Ted Cotterill, operates within the state’s Management Performance Hub (MPH), a standalone state agency charged with fostering data-driven innovation and collaboration among the other agencies. He sees this as an ideal position for the CPO, because it allows the role to add value to efforts happening statewide and send a message that privacy best practices should be considered when using data. That holds especially true when agencies share sensitive data in order to tackle tough challenges, as is the case in Indiana where MPH is coordinating an effort to combat the opioid crisis.

“We realized early on that all of this siloed data maintained by our agencies can provide really valuable insights when leveraged as a strategic asset, and in MPH we’ve been able to create legal, technical and business proficiencies by … [consolidating] this data,” he said.

WEST VIRGINIA: State CPO Ashley Summitt is positioned within the Board of Risk and Insurance Management (BRIM), which offers casualty insurance coverage for state agencies. West Virginia has actually had a CPO longer than any other state, with Gov. Bob Wise first creating the role in 2003. Until two years ago, the position was within the Health Care Authority. But in 2017, with the privacy office focusing more and more on insurance matters, Gov. Jim Justice put the State Privacy Office into BRIM, which is in the Department of Administration.

Summitt said it’s good positioning so her agency can have a tech focus while staying close to its core work. “Privacy cannot thrive without data security, and with the Office of Technology being a sister Administration agency, it gives us a great opportunity to work even more closely together to enhance risk management in these areas,” she wrote in an email.

WHICH AGENCY IS THE CPO IN?

IT department: 9
Other: 2*

WHO DO THEY REPORT TO?

Department head: 5
Chief information security officer: 2
Department deputy director: 1

TITLES

Number of state CPOs with each word in their title:
Privacy: 10
Compliance: 2
Data: 2

* Data was gathered from state CPOs, communications officers, agency websites, LinkedIn profiles and coverage from GovTech as well as other publications. Moriah Sollie helped gather the data. Due to lack of comprehensive staff listings and variance in terminology, it’s possible that there are states with CPOs not included on this list. If we missed one, let us know at bmillergovtech.com.
Eyes Wide Open

NASA engineers are at work building the Mars 2020 rover, slated to land on the Red Planet’s Jezero crater next February. On May 29, they re-installed an important component, the cover to the remote-sensing mast, which carries two Mastcam-Z HD cameras — the rover’s “eyes.” One of the first things the rover will do on Mars is raise the mast, allowing the cameras to do several things: help the machine navigate, allow scientists to better view the materials on the planet’s surface and help them build its geologic history. “Mastcam-Z will be the first Mars color camera that can zoom, enabling 3-D images at unprecedented resolution,” said Jim Bell, Mastcam-Z principal investigator from Arizona State University.

Source: NASA Jet Propulsion Laboratory, California Institute of Technology.
AS CONCERNS ABOUT PROTECTING ONLINE PERSONAL INFORMATION GROW AND LITTLE IS DONE AT THE FEDERAL LEVEL, STATES — AND THEIR IT LEADERS — TAKE BOLD STEPS.

PRACTICAL PRIVACY
In spring 2018, the European nations put into effect sweeping privacy standards known as the General Data Protection Regulation, or GDPR. The move gave consumers far greater control over how their personal information is gathered and used. GDPR also shined a harsh light on the lack of privacy controls here at home. Except in some select cases — primarily in health care and education — U.S. citizens don’t have much say over how the personal information they share with corporations or even government entities is utilized.

Some want the federal government to act, and since that isn’t happening anytime soon, states are beginning to take up the slack. The reason is simple: Americans want more control over their data. A study by technology provider Akamai found 66 percent of those surveyed want the U.S. to adopt GDPR-style rules. Most people think the responsibility lies squarely with government. A recent survey by software provider SAS found 67 percent of those polled said the government should do more to protect their privacy.

Privacy advocates say government should implement some basic requirements. “We want to be sure that people have a right to know what data companies have collected about them,” said Hayley Tsukayama, a legislative activist for the Electronic Frontier Foundation. “We would also like to see the sale or sharing of data be an opt-in activity, where right now it is opt-out. We also talk about the private right of action, that consumers should be able to take companies to court if they violate their privacy rights.”

The issue of data privacy is deeply linked to Internet use, which means it is inherently a component of interstate commerce. That lands it squarely in the jurisdiction of federal legislation — or at least it should. Congress, however, has so far failed to act.

In the current political climate, “the federal government has made themselves functionally irrelevant to so many of the pressing public issues of our day,” said Washington state Sen. Reuven Carlyle. “Even if Congress decided to do this tomorrow, it would still take them five years.”
Rather than wait, Carlyle and other state leaders have stepped up to assert control over what many perceive to be an urgent situation. “That’s as it should be, at least according to some experts in the field. “Where gaps are identified in the laws that aren’t covered by federal regulations, states should have a duty to protect their residents,” said Jay Trinckes, a principal with security consultancy NCC Group. “This includes passing stricter laws on privacy and enforcing these laws to protect their residents’ rights. States should develop guidelines and standards along with providing paths to assurances that organizations should be required to abide by in protecting their consumers’ data privacy.”

In fact, states may be better positioned than federal authorities to move in this complex area. They have flexibility to try new policies and be a little more experimental, according to Aleecia McDonald, assistant professor of practice at Carnegie Mellon’s Information Networking Institute in Silicon Valley. “States can often update laws in a faster, more agile way.”

RAPID TECHNOLOGICAL CHANGE
A case in point is the state of California. When the California Consumer Privacy Act (CCPA) becomes effective in 2020, it will give that state’s residents sweeping new protections. They will have the right to:

• Know what personal data is being collected about them.
• Know whether their personal data is sold or disclosed and to whom.
• Opt out of the sale of their personal data.
• Access their personal data.

They will have the right to:
• Know what personal data is being collected about them.
• Know whether their personal data is sold or disclosed and to whom.
• Opt out of the sale of their personal data.
• Access their personal data.

• Utilize services, even if they exercise their privacy rights.
• The law applies to any business that either has annual gross revenues in excess of $25 million; holds personal information on 50,000 or more consumers; or earns more than half its revenue from selling personal data.

Rapid technological advances made the law necessary, according to state Sen. Bob Hertzberg, who introduced the legislation behind CCPA. “In the old days, privacy was a peeping Tom or somebody getting your mail,” he said. “Today there is the ability to analyze everything about your life, to follow everywhere you go at all times.”

He pointed to marijuana legislation as an apt analogy for privacy rights. Federal government is too big and too slow to move on cannabis, so states have stepped into the breach. With GDPR as a model, states now have a similar opportunity to give consumers greater control over their personal information.

For states that cannot muster the political will to craft legislation on par with CCPA, there is still plenty of room to make incremental improvements, according to Hertzberg. “You can start with the right to tell the companies not to sell your information. You should be able to say, ‘No, it’s my information. You can’t make money off of me,’” he said.

INTERNAL MECHANISMS
Before looking to regulate how corporations leverage consumer information, some chief privacy officers and their partners in state IT are working to ensure that personal data held by the state is handled appropriately. Since becoming the first chief privacy officer of Arkansas in 2018, Jennifer Davis has scrutinized every new piece of legislation to ensure government is not being too heavy-handed with personal data and works with sponsors where necessary.

Recently, Davis reviewed a state plan to adopt monitoring software intended to prevent overbilling on contracts with state agencies. The tool would take screenshots and monitor keystroke activity among contractors who work with the state. “That sounds like a prudent way to manage state funds, but there is no way you can do that without capturing personal data, and we spoke against that,” she said.

To better safeguard privacy, Davis has worked to shrink the data profile across state agencies. She advocated for legislation that cut the governor’s direct reports from 42 down to 15 individuals, with an eye toward streamlining data management. “That will give me 15 people to work with, rather than having to work with all the individual boards and commissions,” she said. “There will be opportunities for greater data sharing, but it will be in a more controlled environment.”
Right now, every state agency in Arkansas sets its own terms and conditions for information use. Davis wants to develop tighter controls that all agencies should follow. “It may mean that you cannot sell this data to others, that you cannot use this data beyond its intended purpose,” she said. “We want those to be consistent across the whole state.”

THE BATTLE FOR A BALANCED PRIVACY LAW

While Davis’ structural initiatives are helping to safeguard state-held data, others who have tried more ambitious projects have been less successful. In Washington state, lawmakers this spring failed to capture enough votes in the House to pass a measure similar in scope to California’s privacy act, even though it passed overwhelmingly in the state senate.

Carlyle’s bill would have given consumers in Washington the right to know what data was being collected and whether it was being sold to third parties. Companies would have been required to let consumers fix inaccurate data, delete personal data and opt out of having their data sold. Opponents alleged that Microsoft and other tech giants had literally helped write the bill and had watered down protections. Carlyle described a year-long collaborative process with industry that eventually won Microsoft’s endorsement of the bill, which he said would have benefited the tech industry as well as consumers. “When you have bad actors, it implodes the ability of the public to have confidence. Everyone should be in favor of having clear lines of authority and accountability,” he said.

While he’s vowing to bring up another privacy bill next year, Carlyle laments that those who advocate for more stringent regulations may be setting too high a bar. “Many in the privacy advocacy community have made the ‘perfect’ the enemy of the ‘good.’ Legislation is by its nature incremental, but many consumer advocates want a categorical approach, a model where all data at all times resides within the power of the individual,” he said. For example, Carlyle pointed to calls for legislation that would apply restrictions and penalties to any business, of any size.

Better, he suggests, to go after the big fish. “What we are looking for is patterns of abuse and systemic issues,” he said. “We are not trying to go after the local grocery store that sends an email inappropriately.”

Even states that restrain their ambitions may face hurdles in trying to regulate data privacy, said Kristina Podnar, author of the new book The Power of Digital Policy. They may experience:

- Pushback from businesses, who see privacy requirements as a burden, and who find it hard to comply with rules that vary from state to state.
- Lack of expertise in defining and enforcing digital privacy.
- Uncertainty about what the legal foundations ought to be for privacy laws. States do not create rules in a vacuum. National and local governing frameworks must also factor in.
- Technical hurdles: States may, for example, rely on Social Security numbers being listed in the memo line of a check to match up payments with taxes owed. New reporting and payment systems may be needed.

WHAT’S THE ROLE OF STATE IT AND PRIVACY?

Even before trying to address commercial practices, states can address data privacy by ensuring proper handling of the information contained in state IT systems. This begins with concepts around data minimization, least privilege and need-to-know access rules.

“You need to bake those into any new solution and push those as a cultural mindset among the government employees, so they don’t get numb to the sheer magnitude of personal information that they see on a daily basis,” said Barbara Symonds, a director in risk advisory services at Grant Thornton. “It starts with that awareness that every single employee is a data steward.”

As legislators look to extend these same safeguards out into the public sector, state IT leaders should have a prominent place at the table. With their technical skills, they will be the ones to implement privacy
legislation on the back end, and should therefore play a prominent role in ensuring that legislation is realistic in its goals.

IT experts “are typically at the forefront of leveraging evolving technologies for securing personal data; they have access to state-of-the-art tools, so they are well positioned to make a valuable contribution,” said Karen Neuman, former U.S. Department of Homeland Security chief privacy officer and now privacy lead at the law firm Goodwin Procter. “They have the expertise and the skill needed to engineer and manage those solutions.”

At the Electronic Frontier Foundation, Tsukayama envisions state IT taking a lead role in the formation of privacy policies. Technology leaders “understand what is fiscally possible and what is technically possible,” she said. “IT can make it clear to the policymakers: If you want this outcome, this is the sort of data we need, and we don’t need this. They can think carefully about what needs to be done, preferably with the least amount of data possible.”

Carlyle puts IT front and center in any major legislative push around privacy. “The need for technical skill in our public-policy work is imperative,” he said, noting that CIOs can play a profound role in leading the development of public policy. “We in the public sector need those with the technical skills to be thought leaders and teachers as we talk about how to manage data better.”

Even with tech experts at the table, privacy is a tough nut to crack. “You can define all the privacy laws you want to have controls in place; you need to have laws in place, you need technology to support the implementation. It will be the ones who bring privacy to life,” Carlyle said.

Privacy experts like former Ontario, Canada, Information and Privacy Commissioner Ann Cavoukian advocate for a default position of “opt-out” when it comes to data sharing.

“Privacy by design” is a foundational model for data management. It says in effect that privacy is the default, that your data belongs only to you and, if you give it away, it can only be used for a specific designated purpose. “Your customers and your citizens don’t have to ask for privacy,” she said. “You give it to them automatically as the default setting; they don’t have to search for the ‘opt-out’ box.”

Such a model helps to build trust: Consumers and citizens have an inherent understanding that there will be strict limits on how data is used and how it is shared. It’s not a model embraced by all, however.

“The lobbyists for Facebook and Google don’t want it,” Cavoukian said. “They might say they do, but really they feel this would curtail their business, which right now involves doing whatever the heck they want with your information.”

The power to hold, share or dispose of personal data should rest with the individual, she says. People should be able to amend or dispose of personal data, use and how it is shared. It’s not a model embraced by all, however.

“The lobbyists for Facebook and Google don’t want it,” Cavoukian said. “They might say they do, but really they feel this would curtail their business, which right now involves doing whatever the heck they want with your information.”

The power to hold, share or dispose of personal data should rest with the individual, she says. People should be able to amend or dispose of personal data, use and how it is shared. It’s not a model embraced by all, however.

“The lobbyists for Facebook and Google don’t want it,” Cavoukian said. “They might say they do, but really they feel this would curtail their business, which right now involves doing whatever the heck they want with your information.”

The power to hold, share or dispose of personal data should rest with the individual, she says. People should be able to amend or dispose of personal data, use and how it is shared. It’s not a model embraced by all, however.

“The lobbyists for Facebook and Google don’t want it,” Cavoukian said. “They might say they do, but really they feel this would curtail their business, which right now involves doing whatever the heck they want with your information.”

The power to hold, share or dispose of personal data should rest with the individual, she says. People should be able to amend or dispose of personal data, use and how it is shared. It’s not a model embraced by all, however.
BEST OF WHAT'S NEW IN INFRASTRUCTURE AND DATA

Platforms and tools for delivering insights and results.

2 A New World of Infrastructure Options
4 The Power of Breaking Down Data Silos
6 Supporting a Culture of Analytics Through Self-Service
8 Using AI, ML, and Other Emerging Technologies to Protect Data and Infrastructure
10 Using the Right Tools and Approach to Leverage Data Strategically
12 Flexible, Sustainable Data Solutions Start with the Right Platform
14 Creating Visibility Across Today's Complex Infrastructures
16 3 Tips for Hybrid Infrastructure Success
Last year, Oakland County, Mich., used the cloud to ramp up the capacity of its election system, ensuring ballots were processed efficiently during a busy election season. Once the election was over, system capacity was dialed back down. For Phil Bertolini, deputy county executive and CIO for Oakland County, the cloud was a practical way to address the temporary spike in volume. “Why should I architect an onsite data platform to handle peak demands when a large percentage of it would be underutilized during the rest of the year?” he asks. Flexibility and scalability are just a couple of the reasons why cloud-based solutions handle a growing percentage of Oakland County’s computing workload. Bertolini says about 20 percent of IT operations are in the cloud today, and that number could grow to 50 percent within three years. Oakland County isn’t alone in turning to the cloud. Recent Center for Digital Government (CDG) surveys found that although the bulk of state, city and county respondents have 30 percent or less of their computing workloads in the cloud today, they expect those numbers to grow to 50 percent within three years. Twenty-nine percent of respondents said their jurisdictions use three to five cloud environments across all departments, making it the most common answer. Another 13 percent said their jurisdictions operate more than 10 cloud environments.

Preserving the Data Center
Clearly the push in government is toward more cloud — but not necessarily all cloud. The flipside of the CDG survey results is that a significant number of state and local IT leaders see less than half of their computing workloads moving off-site. The rest will stay put. “The long-term trend may be to move more and more services to the cloud, but many CIOs will stay with a hybrid environment for the foreseeable future,” says CDG Executive Director Teri Takai. “They feel they can better manage the costs and performance of certain functions by running them in their data centers.”

Fortunately, on-premises data center technology is improving too, often providing “cloud-like” advantages through the traditional hardware ownership model. One example is hyperconverged systems, which tightly integrate computing, storage, networking, virtualization and IT management resources into a single unit to simplify infrastructure management and integration. In the state of Louisiana, hyperconverged technology is the foundation for a project to modernize the state’s Medicaid system and provide single sign-on capabilities. In addition, hyperconverged equipment in the state’s two main data centers in Baton Rouge mirror each facility’s capabilities, enabling automatic failovers to reduce downtime and strengthen business continuity. Derek Williams, director of Louisiana’s state data center operations, says the hyperconverged computing environment — which lets his IT staff plug in additional appliances to increase...
Government Goes Hybrid

Putting It All Together

For IT leaders, this new hybrid, multi-cloud world offers more infrastructure options than ever before. Organizations have unprecedented ability to match applications and workloads to the right computing models, cost structures, security levels and more. At the same time, managing and securing this complex new environment demands new tools and skills. Agencies will also need a firm grasp on current computing costs, data classification and a host of IT governance issues to make smart choices among an ever-widening array of alternatives.

Getting the most benefit from hybrid IT requires leaders to assess current applications, prioritize those most in need of modernization and then choose the appropriate computing platform. Factors in cloud versus on-prem decision-making include an application’s dependency on other data center systems, as well as its performance and bandwidth requirements. For instance, transferring large quantities of high-definition video in and out of cloud-based platforms can be expensive and taxing on enterprise networks.

Security and privacy requirements also may dictate whether data can be moved to the cloud and what type of cloud platform can be used. State laws may limit where data can be housed, for example. And sensitive material like FBI Criminal Justice Information Service (CJIS) data or patient files protected by HIPAA may demand specialized government cloud solutions that offer appropriate security configurations — usually at a higher price than standard public cloud services.

Intelligent tools will also be another vital part of the hybrid equation. Agencies will need a new generation of management solutions that give IT teams visibility across those sprawling infrastructures and automate labor-intensive software updates and patching processes. They’ll also rely on sophisticated security solutions designed to protect attack surfaces that now span from the data center to the cloud. And increasingly powerful analytics packages may be necessary to monitor system performance and traffic patterns, enabling IT staff to make adjustments that optimize user experience. Together these tools will help IT leaders improve the security, reliability and user acceptance of hybrid environments while reducing demands on overworked public sector IT departments.

Ultimately, state and local government IT leaders need to create hybrid strategies that take advantage of rapidly expanding cloud-based innovation while continuing to modernize important data center technologies. And just as important, successful organizations will implement the vision, policies and tools that enable them to optimize these pieces and run them as a cohesive whole.
THE POWER OF BREAKING DOWN DATA SILOS

What’s the difference between artificial intelligence and augmented intelligence? On the surface, augmented and artificial intelligence look alike with one major difference — there’s a person, likely a developer, behind augmented intelligence telling the program how to learn. Augmented/cognitive technology is designed to enhance human intelligence, not replace it. People should think of augmented intelligence as a complement to human intelligence. It’s about helping humans become faster and smarter at the tasks they’re performing.

On the other hand, artificial intelligence is often implemented today as a mechanism of automation that is machine learned and enhanced. We believe human and machine intelligence need to be connected with context.

Why should government organizations embrace augmented intelligence and machine learning? Agencies have made significant investments in big data platforms to collect data, but it’s difficult for non-technical personnel to extract valuable insights from these platforms. The good news is agencies can now leverage this data by using augmented intelligence to reduce the barriers and expertise required to gain insights. To do this, however, agencies must solve significant data availability challenges.

Gemini enables public sector teams to use a unified SQL query across multiple data platforms without copying, moving or transforming the data. This provides data availability that must be at the foundation of every digital transformation initiative. Data availability also delivers the data diversity needed to make artificial intelligence a reality. What challenges do state and local governments encounter when they move to extract greater value from their ever-expanding infrastructures? We believe extracting more value from an ever-expanding data infrastructure is basically unattainable. And the sad truth is, according to McKinsey, most digital transformation initiatives have failed to meet expectations due to data and organizational silos. Over the past two decades, public sector organizations have evolved their analytics architectures from databases, to data warehouses, to data marts, and now data lakes. These organizations sought easy access to data, data reuse, tight integrations and simple deployments. Unfortunately, this vision didn’t pan out. In reality, these public sector organizations built more silos, lakes and proprietary data platforms.

How can organizations eliminate the complexity of using augmented intelligence to meet their mission and better serve citizens? Gemini eliminates complexity in three ways. We make data easily available for artificial and augmented intelligence. We provide a single query language for use on data residing in some of the most complicated data platforms. In addition to SQL, Gemini helps lower the skills barrier by making data access and availability simpler across complex systems that contain critical data. How can augmented intelligence solutions help address the shortage of data scientists and analysts within government agencies? Augmented intelligence seeks to empower teams with faster and smarter decision-making. Conceptually, this makes a lot of sense. In reality, until an organization addresses its data availability challenges, augmented or artificial intelligence is basically unattainable.

Once this issue is addressed, data is made available quickly and easily and the power of augmented intelligence is unlocked for many more users, which will help alleviate gaps caused by the shortage of data scientists. Gemini includes Unified Data Access using ANSI-SQL, the world’s most adopted query language for use on data residing in some of the most complicated data platforms. There are a lot more SQL experts in the market than specialized systems experts. In addition to SQL, Gemini helps lower the skills barrier by making data access and availability simpler across complex systems that contain critical data.

Learn more at CarahJ.io/Gemini-Data
Demystify your Digital Transformation Journey with Data Availability

**Access**

your data silos, lakes and warehouses without ETL, moving or copying data.

**Connect**

machine and human intelligence to deliver enterprise knowledge.

**Consume**

the full context of your data and explore relationships with greater insights.

geminidata.com
Where do you see the biggest potential for state and local agencies to leverage data coming from today’s expansive infrastructures to improve performance and service delivery?

The biggest potential — and the biggest challenge — is instilling an expectation that an organization’s data will be leveraged for all key decision-making. In other words, it’s about creating a culture where it is a given that data can and will be put together accurately and quickly to explain what has happened and predict what will happen next as part of all critical policy decisions. If this kind of data-driven culture is adopted and supported by an analytic service that delivers timely and insightful information, then the potential is enormous to vastly improve services across all aspects of government, including health services, transportation, public safety, utilities and more.

What key challenges do agencies face when trying to use data more effectively?

There is a massive shortage of true data scientists, who are traditionally thought of as necessary to establish a culture of analytics. To address this, agencies are empowering their existing line-of-business workers to become citizen data scientists. These workers understand their data, and we shouldn’t sell them short. Instead, organizations must enable them to use their data and bring it together with other data, all in an approachable self-service process that doesn’t require a data science degree or coding capability.

How can self-service data analysis help agencies use data and business intelligence to deliver services quickly, intelligently and cost-effectively?

Traditional data analysis involves many steps before data or insights reach decision-makers, and these steps frequently involve multiple teams. Self-service data analysis streamlines this process and makes advanced analytics more accessible. Workers at all levels can grab data from any source, in accordance with security and permissions policies, and then curate and normalize that data themselves. This approach creates massive savings and greatly reduces the time to deliver insights.

What advice do you have for IT and business leaders as they get started with (or advance the use of) data analytics in their organizations?

Establishing a culture of analytics is a journey. Instead of beginning with a large, wide-sweeping RFP, identify quick wins. Engage line-of-business workers to quickly drive specific answers to typical issues. Find low-hanging fruit those workers can go after and give them user-friendly tools so they can perform their own analysis. A lot of times that starts with the creation of an analytics app. Grow from there to enable other stakeholders to experience the use of data across the organization. Finally, to build momentum, start putting predictive models and other advanced analytics into employees’ hands and consider reusing analytics components to scale across departments.

Learn more at Carah.io/Alteryx-Data
BUILD A CULTURE OF ANALYTICS

WITH A MODERN, SELF-SERVICE PLATFORM

• Level up analytics efficiency, not headcount
• Scale insights across departments
• Deliver vital digital + cultural transformation

VISIT THE ALTERYX PUBLIC SECTOR SOLUTION SITE AT WWW.ALTERYX.COM
What challenges do state and local governments face in securing data and infrastructure as they move beyond traditional data center models?

We think about risk in terms of threats, vulnerabilities and assets. State and local governments provide a lot of critical infrastructure, and they have non-public personal information that is very attractive to adversaries. As for vulnerabilities, their infrastructure tends to be dated and frail. Much of it is decentralized, so there’s poor visibility into vulnerabilities. In addition, it tends to be non-segmented, so once adversaries get inside the infrastructure, they can go wherever they want. In terms of threats, adversaries can now automatically scan the internet for opportunity. Because government infrastructures have such a large attack surface with many entry points, threat actors can often find a way in. When it comes to mitigating these risks, organizations often don’t have the talent or can’t scale to defend such a large, diverse environment.

How can a managed security service (MSS) help agencies meet these needs?

There is no faster way to improve your cyber maturity than to hire someone who does this day in and day out. An MSS provides a very skilled labor force that helps organizations fight threat actors and adversaries, reduce the attack surface and mitigate vulnerabilities so that if an attack occurs, exposure is limited. An MSS also helps identify and prioritize assets in your environment so you can focus on defending the most critical assets.

How can AI and ML improve threat intelligence and security services overall?

With AI — and machine learning, in particular — instead of us having to continuously tell the system what’s malicious, the security monitoring systems themselves are gaining the capability to tell us what they think is malicious. That software-driven versus people-driven approach enables speed and scale and is an extremely important pivot point for the security community overall.

What other emerging technologies will help agencies improve their security posture?

There are a lot. Software-defined data centers provide greater visibility, so you can see the network and its assets and then understand what terrain needs to be defended. Sensing capability that allows monitoring is also really important to gain visibility into the infrastructure and detect availability, integrity and confidentiality issues. Lastly, federated machine learning is going to have a huge impact on defending municipalities. That means taking what you’re learning from one infrastructure, from a security perspective, and applying it to defend another infrastructure; so once one city or region is hit, you can automatically learn from that compromise to help inoculate or defend other areas.

What advice can you give for integrating ML and AI into an organization’s security strategy?

First, identify a specific security use case and then decide whether data science or ML can help you in that use case. Avoid trying to impose data sciences simply for the sake of using them. Second, rich data and simple algorithms win the day, so be cognizant of the quality and breadth of your data. That’s more valuable than trying to infer or guess something because you don’t have a piece of data. Lastly, computer security personnel usually aren’t data scientists. It takes someone with data science capabilities to generate the algorithms needed for true machine learning.

Conversely, software developers or data scientists are not cybersecurity experts. In order to create and apply cybersecurity analytics effectively, you need to know what the security use cases are, determine what data you need and identify what data sciences techniques will provide the most value.
Secureworks®

Detect faster, respond smarter, and predict and prevent more threats altogether.

Learn more about Managed Detection and Response Services at https://carah.io/SecureWorks-5-16
Where is the biggest potential for state and local governments to leverage data to improve performance and service delivery?

**Kieran Taylor:** The biggest potential is to transform government by bringing all data and processes together to get a unified view of the user experience and deliver value in the moment — whether that data is on-premises, in the cloud or in the mainframe. There is also great potential for leveraging AI and machine learning to offload some of the more common manual tasks related to this data and data processing and get to actionable insights more quickly.

What key challenges do state and local governments face when building or expanding their infrastructures to accommodate new sources of data?

**Kieran Taylor:** We sometimes refer to this as the four Vs: variety, volume, velocity and veracity of data. How do you assimilate a wide variety of data formats? How do you process a high volume of data? How do you keep up with the velocity of change and very ephemeral infrastructures? How do you know that data is accurate and can be trusted?

How can organizations approach infrastructure modernization and expansion to take advantage of all the data coming in and deliver services quickly, intelligently and cost-effectively?

**Chip Mason:** It’s critical to understand the benefits of the technologies being considered and leverage the appropriate infrastructure for the task at hand. In our experience, a hybrid approach that uses each technology for what it’s best at is often the most successful — whether it’s using the mainframe for its exceptional connectivity, using the cloud for its ease of use, running portions of cloud or big data projects on-premises, or doing some portions in mobile and having back-end data systems do the calculations. We now have advanced API tools and accessibility standards that can help organizations easily develop interfaces between older systems such as mainframes and the tools and services they want to provide — whether they are cloud, mobile or something else. These tools often provide a quicker, simpler way to leverage what the organization already has.

What advice do you have for agencies as they modernize and expand their infrastructures to enable the collection, transmission, storage and analysis of data coming from edge computing, cloud and other emerging models?

**Kieran Taylor:** First, locate all the data collection points in your digital delivery chain; understand how you can get access to the data and how you can get the data into a central data lake where it can be normalized. Second, implement technologies such as AI and machine learning to improve access to and processing of the data. The more advanced out-of-the-box AI and machine learning solutions can automate common remediation and optimization tasks, and therefore speed up the rate of transformation.

**Chip Mason:** I would add there is also an inherent cybersecurity risk when you’re moving data around and don’t know exactly what the content of the data is or its sensitivity. It’s important to conduct a thorough analysis before moving that data.

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

Copyright © 2010 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.
How are government agencies evolving in the way they collect, transport, store and analyze data?

Henry Sowell: Agencies recognize they have to think beyond their own single silos of information and may need to onboard many different data sources. So they’re looking for ways to move and store data more simply. They’re also looking for advanced ways to analyze the data they’re bringing in.

Marcus Waineo: We’ve seen a definite shift from users having a single analytics tool they were trained on and have been using for a long time to a more refined need for multiple analytic tools, in multiple languages, with people bringing different backgrounds and skillsets to bear to analyze the same data.

Why do organizations need a new approach to become data-driven?

Henry Sowell: For a long time, people have made decisions based on their “experience” and going on their gut instinct of what they expected to happen — and suffering from the impact of the mistakes that can come from that. We’ve gotten to the point where we no longer need to operate that way. We can actually leverage the data we’ve collected over an extended amount of time to make more informed decisions. Beyond that, we can also start to make predictions about what may happen based on the data we have received. That’s key in helping organizations make more effective decisions to support their missions.

How does an enterprise data cloud platform enable organizations to take advantage of data they collect to deliver better services?

Marcus Waineo: The idea behind the enterprise data cloud platform is to run systems where it makes the most sense to run them. So it’s taking advantage of the geographic distribution of the cloud as well as the ability to elastically scale in the cloud to deliver services where they’re needed, in the quantities they’re needed, and with whichever cloud service provider is needed.

Henry Sowell: It also allows organizations to choose a hybrid cloud approach, where they can run some workloads on-premises while still having the flexibility to scale into the cloud and manage across those different areas.

What can organizations do to ensure governance and security in this new environment?

Marcus Waineo: Organizations should be looking for technology that enables a consistent governance and security posture across infrastructure and across infrastructure providers, while also protecting against vendor lock-in. That speaks to the core hybrid cloud architecture approach as well as the multi-cloud architecture approach. You need technologies that ensure governance regardless of where the workloads and data reside. Similarly, you need a consistent approach to security regardless of which cloud service provider or on-prem environment is being used.

Learn more at Carah.ii/Cloudera-Data
Realizing the Enterprise Data Cloud from the Edge 2 AI

coudera.com
What IT management challenges do government agencies face as infrastructure expands beyond the traditional data center and into co-location, hybrid cloud and other new environments?

One challenge is related to staff training and the accelerating pace of change. If an agency’s IT staff doesn’t keep up with the core technologies that are emerging, and if they don’t have the proper technical skills, they won’t be able to effectively leverage the newest technologies to better serve constituents. In addition, the organization will face greater risk in terms of both security and project management. Another challenge is around visibility and tooling. As organizations move workloads beyond the traditional data center, the ability to connect end to end becomes more challenging. As a result, organizations lose visibility into how those assets are performing.

What risks should state and local government leaders be thinking about when incorporating new sources of data and technologies into their infrastructures?

Stability and security. When infrastructure is evolving rapidly, it’s more difficult to have a stable, highly available platform if you’re not aware of how changes will impact you. SaaS and services vendors may be pushing code changes weekly or even multiple times per day, and those changes may impact something you have built technology on top of. To ensure platform availability, it’s critical to thoroughly understand the change control process of whichever vendor(s) you’re using. Regarding security, once you start bridging infrastructure components to create a hybrid cloud, risks expand greatly. If you’re moving really fast and security is not top of mind, you might build something that is highly functional but it may expand your risk exposure; you have to be very intentional and pragmatic when you think about securing your infrastructure in a hybrid world.

How do enterprise-level management and monitoring tools help simplify the operation of these complex new infrastructure environments?

The key is to create visibility across the entire infrastructure, whether something is on-prem, pure cloud or hybrid. With everything so distributed today, it’s much more difficult to isolate problems because there are so many interdependencies. Enterprise-level management and monitoring tools help simplify operations by providing clear visibility into the expanded infrastructure, its interdependencies and the location of potential problems.

How can organizations best use management and monitoring tools to meet current demands while also creating a path to the future?

Most government entities can’t just bulk replace everything. There is a long tail of technology and legacy applications that they’ll have to support for a long time. To future-proof their monitoring strategies, organizations must ensure they can bring the full scope of both legacy applications and the new modern applications into view — all in a single pane of glass that allows them to see all the services they’re delivering. Some vendors focus on the newer technologies and don’t address legacy technologies. It’s critical to work with a well-established vendor that understands these things and can tie the whole infrastructure together.
Solve your toughest IT management problem, today

Scalable, end-to-end IT monitoring software from solarwinds.com/government
As CIO for the city of Minneapolis from 2011 to 2018, Otto Doll had a front-row view of the evolution toward hybrid and multi-cloud IT.

“It takes hundreds of applications to run a city or a state today,” says Doll, who is now a senior fellow for the Center for Digital Government. “But the things you’re responsible for aren’t just in your data center anymore. That creates new challenges around governance, how you deliver applications, data privacy, etc.”

Doll recently shared his thoughts on how to thrive in today’s rapidly evolving infrastructure environment:

1. **Fully evaluate how and when you’ll need to pull data from the cloud.** Moving data in and out of the cloud can be difficult and expensive. Negotiate with your cloud providers to ensure you can transfer data out of your cloud environments for analytics or other needs without incurring large costs. “If you don’t pull your data out of the cloud at some point, you’re just putting your legacy data silos into cloud silos,” says Doll. “At certain points you’re going to want to aggregate data from various places to evaluate operations and look for ways to improve city management.”

   For example, when Minneapolis implemented a cloud-based 311 system, city leaders realized data from workorders they received could be used to spot emerging infrastructure problems and other issues. But until they could pull that data out of the cloud for further evaluation and comparison with data from other systems, they couldn’t see the larger problems they needed to address.

2. **Understand the true cost of on-prem, cloud or hybrid.** There’s no silver bullet when it comes to infrastructure. Determining the best option depends on multiple factors. “It’s a game of determining if you’ll be transitioning enough work into cloud to make it competitive and give you the type of ROI you need, or whether some things are better left on-prem,” says Doll.

   At the same time, government IT leaders are under constant pressure to react to “better deals.” But those deals can come at a price. For instance, private sector rules and processes don’t always fit how government works. If a solution requires departments to drastically change the way they do business, it may not be as cost-effective as expected.

   “A lot of government apps and business rules are unique, so a cloud-based solution that fits our needs might not exist,” says Doll. “One of the factors you have to weigh as a CIO is whether or not you can or should make business changes to move to a new platform.”

3. **Think from the inside out.** At the end of the day, infrastructure exists to empower your workforce. Designing infrastructure from the end user’s perspective can arm city workers with tools that enable them to work as a team. For example, giving technology to police officers or other mobile employees that makes it easier for them to report problems like a leaking fire hydrant or broken street light can ultimately improve citizen services and quality of life.

   “Technology can have that kind of impact,” says Doll. “We just need to convince people that shifting the approach is worth the effort and the money.”
FACING THE FUTURE

THANKS TO MASSIVE GAINS IN ACCURACY AND LOWER COSTS, FACIAL RECOGNITION IS BETTER THAN EVER. BUT IS THE TECHNOLOGY A THREAT TO OUR PRIVACY?

BY TOD NEWCOMBE
In 2017, the Washington County Sheriff’s Office in Hillsboro, Ore., became one of the first law enforcement agencies in the country to use Amazon’s facial recognition software program, known as Rekognition. 

Powered by the latest in artificial intelligence, the tool allows Washington County officers to look for matches of a suspect’s face by quickly sorting through more than 300,000 mug shots in a county database that goes back to 2001, according to a report in The Washington Post.

Sheriffs have used facial recognition more than a thousand times since the program was installed more than 18 months ago, and the software has led to dozens of arrests for theft, violence and other crimes, according to the Post, but its use has also raised some red flags among privacy advocates who question its accuracy, especially for individuals with dark-skinned faces, and how the police decide to use the technology.

The facial recognition market is growing rapidly ($7.76 billion value globally by 2022, according to the research firm Markets-and-Markets) as demand for surveillance, monitoring and identity grows. But as the technology becomes increasingly accurate, it could further diminish what privacy we have left, say critics. That has set off alarm bells, demands for stricter regulations and laws on how and when it should be used, and, in some cases, outright bans.

ALGORITHMS GROW UP

Biometric identification technology has been around for decades. Fingerprinting became a high-tech, automated process with the development of automated fingerprint identification systems (AFIS) in the 1980s. In 1999, the FBI launched a nationwide version of AFIS, which now contains fingerprints from more than 143 million individuals. During the same period, facial recognition technology began to emerge, thanks to some early generation algorithms that could map a subject’s facial features and measure differences between faces that the computer can compare in a database containing thousands, even millions of images.

Because of limits in computing power and the lack of sophistication with the algorithms, facial recognition was not considered a versatile, practical tool. But that has changed in recent years. “There have been a number of recent advances in face biometrics, primarily in its accuracy, thanks to new, breakthrough technologies,” said Daniel Asraf, senior vice president of Biometric Identity Solutions at Gemalto, part of Thales, a French multinational firm.

The breakthrough has been in the field of artificial intelligence, which has grown rapidly in strength and performance. So-called convolutional neural networks have led to “massive gains” in accuracy in the past five years, according to the National Institute of Standards and Technology. “Prior to neural networks, existing technology just couldn’t reach the accuracy needed to make facial recognition versatile and useful,” said Asraf. “But the neural networks of today are like an offshoot of the brain, giving them a unique ability to recognize images.”

Asraf believes two other factors have contributed to the rise of facial recognition: more computational capacity, which means the algorithms can run on silicon chips tailor-made for faster processing; and better optics and sensors that can render images at extremely high fidelity. “We have much better cameras that can capture images in huge variations of environmental conditions, compared to the resolutions available a decade ago,” he said.

Yet another factor that has boosted the rapid growth is cost. “The price points on supporting technologies — cloud, processing power, memory — are much cheaper than they were 10-15 years ago,” said Benji Hutchinson, vice president of federal operations for NEC’s Advanced Recognition Division. When Amazon rolled out Rekognition, it was as an easy-to-use tool that does not require a heavy investment in hardware, and is available at very low prices. Washington County’s Sheriff’s Office pays about $7 a month for its image searches, according to the Post.

IDENTIFYING IMAGES ON THE FLY

In the early days of facial recognition, limits on algorithms, computing power and

“Neural networks of today are like an offshoot of the brain, giving them a unique ability to recognize images.”

— Daniel Asraf, Gemalto
U.S. Customs and Border Protection plans to use facial recognition for more than 97 percent of commercial air travelers by 2022.

other capabilities meant that using the tool required humans as much as computers. “You had human testers who upgraded the algorithms in a very tactical way,” said Hutchinson. “Humans would record whether or not matches worked well, and then they would tweak the algorithms accordingly.”

Today, that work is all done by computers. The data sets of images are also much larger and, when combined with AI, make the algorithms much more robust, explained Hutchinson. The result is facial recognition that can work from less-than-perfect images. “Facial recognition used to need a fairly pristine image to get a good match,” he said. “Today, that’s not the case.

The images you are checking against in a database can be off-angle, even a profile.” This capability has led to the point where certain facial recognition systems can work in real time, identifying images on the fly. With performance like that, facial recognition has become a much more versatile way to identify images of people. And, with the growth in image databases, the technology is no longer a highly specialized, expensive tool that only a few agencies and organizations can afford to use.

Matthew Zeiler, founder and CEO of Clarifai, an AI firm that specializes in visual recognition, says that as the technology has improved, the number of use cases has grown, particularly in the private sector, where certain industries, such as hospitality, use it to tag images so they can be easily found by computers. It is also being used to automatically filter out unwanted online content, such as drugs, weapons and nudity. Globally, many countries are beginning to use facial recognition for airport and hospital security, while the military is putting the technology into drones that fly over battlefields.

A GROWING MARKET IN GOVERNMENT

For the public sector, advances in facial recognition technology have opened the door to uses in a variety of fields. Zeiler said his firm has worked with agencies and organizations that would like to use
Clarifai’s platform and tools to find and identify people during natural disasters, such as tornadoes, hurricanes, floods or fires. “In these scenarios, when it might not be safe or possible to send humans into the disaster area, drones equipped with cameras using facial recognition might be able to identify specific people,” he said.

School systems have shown interest in the technology as a way to provide security in an age where school shootings have become a grim reality. Departments of motor vehicles, which receive thousands of photographs on a daily basis, can use facial recognition to detect whether the applicant is in the database under another name to evade a driving ban. Correctional facilities are also using the technology as a way to monitor the location of inmates.

But law enforcement remains the prime sector in state and local government for facial recognition technology. According to the IJIS Institute, a nonprofit alliance of tech firms working in the public sector, the technology is typically used by law enforcement to help identify a face against a known image. Sometimes called one-to-one analysis, this identification would involve using facial recognition to ascertain whether a person presenting an image embedded in a passport or driver’s license is the same person. Police also use facial recognition to compare the image of a face to numerous known faces within a database. This function is called discovery and is sometimes referred to as one-to-many analysis.

Washington County’s Sheriff’s Office is just one of a small but growing number of law enforcement agencies that are using the latest generation of facial recognition technology. The Orlando, Fla., Police Department announced last year it would begin testing Amazon’s software before recommending it for broader use. Besides Amazon, Gemalto and NEC, a sizable number of firms have entered the market, many with solutions geared for the law enforcement community. They include: Brainchip, Cognitec, Ever AI, FaceFirst, Idemia and Suspect Technologies, to name a few.

One notable firm that has stepped back from using its facial recognition software for police work is Microsoft, which recently rejected a California law enforcement agency request to install the company’s software in police cruisers and bodycams out of concerns for human rights. Microsoft’s sensitivity about how its technology might be used without proper checks and balances in place reflects the dilemma police departments face in terms of advancing crime fighting prevention using the latest technology that has the potential for abuse, intrusiveness and invasion of privacy.

Rick Myers, executive director of the Major Cities Chiefs Association, which is composed of the police chiefs from the 68 largest cities in the U.S. and the nine largest cities in Canada, is well aware of that quandary. When it comes to technology, police have learned to move with caution, given their unique role and the need for trust when it comes to protecting the safety of communities. Myers cited the example of gunshot location technology. “A few years ago, it showed great promise, but the number of false positives was quite high,” he said. “Over time, a small number of agencies that were early adopters of the technology provided feedback to vendors, who improved the technology, leading to more widespread adoption today.”

Myers described facial recognition as early in its maturation phase. Citing concerns about the inability of some facial recognition technologies to discern people of color accurately, as well as other skin types and facial shapes, he emphasized that the law enforcement community can’t afford...
any technology that has an inherent bias. “On the other hand, we see great potential for facial recognition and other types of artificial intelligence to really expedite our ability to identify high-risk subjects, potential terrorists or serial criminals, prior to them committing another offense. That’s a highly desirable quality,” he said.

A GROWING CHORUS OF CONCERNS

In May, San Francisco, with the blessing of the mayor and city supervisors, banned city use of facial recognition technology. Oakland is also looking to enact a similar ban. In January, a bill was filed in the Massachusetts Legislature for a statewide ban on the use of facial recognition by state agencies. The state of Washington tried, but failed, to pass a privacy law that hinged on putting strict limits on the use of facial recognition.

With stories coming out of China, where the use of facial recognition has become widespread and has been used to suppress ethnic minorities, the chorus of concerns about the use of facial recognition and its ability to strip away any semblance of privacy has grown louder. “The examples of legislative and regulatory pushback against the technology have tech firms and law enforcement officials worried. Gemaalto’s Asraf believes the answer to the problem is for the tech community and government to deliver a combination of good governance and better education. “As a technology provider, we provide the tools for facial recognition, but there’s a second piece and that’s the governance of that, which the government whom we provide the tools to, needs to adhere to,” he said. As for education, Asraf called it a very important piece of how facial recognition can advance, “because there are so many misrepresentations and misconceptions about the technology.”

Myers, who has four decades of experience as a police officer and chief, has seen privacy groups attempt to stifle other technologies considered too intrusive for law enforcement. “It can take years to learn where the boundaries are with regards to emerging technologies that can benefit both law enforcement and communities,” he said.

Myers points out that the police operate within the confines of the U.S. Constitution, which provides individuals with protection against government intrusion into a person’s life. “However, what gets lost in the discussion is that there is no expectation of privacy in a public place, where you are likely to be on CCTV anyway,” he added. Myers sees benefits to using facial recognition in public spaces, along with AI that can analyze human behavior, to help police thwart a possible crime before it occurs or the actions of a terrorist, for example.

A 21ST-CENTURY TOOL

One possible public use of facial recognition in the near future could be at a large event such as the Super Bowl. If evidence suggests someone may have plans to bring a dirty bomb to the football game, cameras with facial recognition technology could be set up around the perimeter to try to identify known suspects. Such a system would have to be able to search and identify someone in real time. It’s one of the future uses of the technology.

“We have the technology today to conduct real-time facial recognition in the field using body cameras,” said Asraf. “With the rollout of 5G, we can expect to see the use of facial recognition in an edge computing environment with real-time feedback.”

Clarifai’s Matt Zeiler also sees edge computing giving facial recognition a significant boost in capabilities. Beyond that, the accuracy will continue to get better as the algorithms get stronger and faster, thanks to ongoing improvements in processing speed and optics that will deliver astounding resolution. “Better accuracy is a no-brainer,” he said.

Benji Hutchinson of NEC perhaps put facial recognition’s future in the best perspective. “It truly is a 21st-century tool.”

Facial recognition used to need a fairly pristine image to get a good match. Today, that’s not the case.
— BENJI HUTCHINSON, NEC
For a certain type of technology company, collecting individualized data has become a business liability. It seems antithetical to the usual narrative, to the idea that data is the new oil and those who can find ways to mine it will get rich quick. Indeed, this largely remains true in the private sector. In government, however, an opposite notion has begun to take hold: With citizens increasingly aware that new and smaller technologies are able to record, monitor and identify their activities, many agencies now insist that the products they buy avoid storing personalized information. In other words, collecting too much or the wrong kind of data can cost these businesses their customers. At least, so say a handful of gov tech companies. Their products are diverse — ranging from recording equipment able to detect gunshots to sensors on benches that count sidewalk traffic — but their approach to data is the same: All collect information and must serve a specific mission without storing personal info that could be used to identify individuals.

The reason for this is simply that communities across the country demand it, and if the people are not OK with a product, government won’t — or perhaps, can’t — buy it. With all of that in mind, let’s look now at these five companies, the products they sell and the precautions they have installed to ensure that citiernes nationwide are comfortable having them in their communities.
1. Only store aggregated data

Moovit is a mobility-as-a-service (MaaS) provider, which means the company offers cities and transit agencies a full suite of transportation-related tools that provide info about how people consume mobility. Yovav Meydad, the company’s chief growth and marketing officer, said that Moovit has the world’s largest transit data repository and multi-modal trip planner. As Meydad is proud to point out, the ride-share company Uber is using Moovit to start to incorporate public transit info into its own app. Microsoft, meanwhile, is another Moovit user, harnessing its MaaS capabilities to aid any internal developers who want to add location-based services to things like trip-planning apps. Moovit is, essentially, in the business of knowing how people move through cities, and it has been since it was founded seven years ago. At that time, it offered little more than a free public transit app, one that needs to track users’ locations to function, a capability that commonly raises privacy concerns.

“We choose not to require the users to create a personal account. Users with Moovit don’t need to provide any personal information, not name or gender or age.”

Basically, Moovit foresaw that people would not want their individualized data shared all over, and so the company took itself out of the data collecting game. Moovit can’t share or lose individual data, because the way its products work, it never collects that info in the first place. Instead, Moovit only stores analytics related to transit usage, doing so in an aggregated fashion.

This is a concept that came up repeatedly among other companies as well: aggregating data and avoiding any identifying characteristics. While it might limit companies like Moovit’s ability to sell user-specific data, it keeps them on the

THE PRICE OF DOING BUSINESS
right side of governmental privacy regulations while also making them acceptable for concerned community members.

2. Aim for privacy by default

RoadBotics comes from a simple-yet-grand tradition of gov tech companies: Its core mission is to use new tools to do an old task better.

In this case, that old task is surveying roads. For many years, government agencies have decided which roads to fix based on a manual methodology that involves people going out to the roads in question, looking at the pavement and rating it on a scale. This is, of course, an inherently subjective process. What RoadBotics does is remove that subjectivity.

The company does this by enabling public servants to mount a smartphone on a passenger-side window to take stock of roads in need of repair. As they drive around, the phone records the roads. At the end of the day, the user connects to a Wi-Fi network, the recorded data is uploaded to secure cloud storage and image processing technology objectively evaluates the road conditions, said Ryan Gayman, the company’s vice president of partnerships.

RoadBotics protects privacy within its products by obscuring the faces and vehicle types that might inherently get caught in its efforts to record the roads. The company’s tech only leaves the roads clear, hurting the people and cars so extensively that someone reviewing the footage wouldn’t be able to so much as guess make or model, let alone the identity of an individual.

With clients in 12 countries, RoadBotics is sometimes required to do this by regulations, but even in places like the United States where such specific protections are yet to be codified, Gayman said the culture demands that privacy be protected.

“Even if it’s not a regulation, people care about privacy,” he said. “So, we have to go above and beyond in that respect.”

RoadBotics is engaged in image processing, a field that has vast potential to improve governmental functions. In order to do so, however, the residents of communities must once again be OK with it. RoadBotics’ approach is to ensure this by being transparent and thorough with the efforts it takes to avoid collecting individualized data. It’s not alone in this respect.

3. Align your mission with the public interest

ShotSpotter sells a complex product that involves dozens of sensors capable of recording audio in service of a simple goal: alerting police in real time to gunshots fired.

One of the points made by all five of these companies was that companies that collect data are best served by having a specific mission that the public can get behind and support, such as rapidly identifying when a shooting has occurred. ShotSpotter certainly has that.

Its operations place audio sensors in areas where they are deployed at a density of 20 to 25 sensors per square mile, which is relatively thin. They are also placed high above the street. This combo of height and sparsity makes it difficult for them to home in on conversations, which is the prevalent concern when it comes to audio products and privacy.

“We’re listening, but we’re listening for gunshots, we’re not listening for conversations,” said Sam Klepper, the company’s head of marketing and product strategy.

What’s more, the only time an actual human listens to ShotSpotter’s audio is after its recording system has clearly identified a loud and sudden noise with a high probability of being a gunshot, Klepper said. Even after a potential gunshot—a noise that is exceedingly loud, brief and sharp—is detected, a human first looks at a visual of the sound, like one might see police monitoring in a TV show or movie. That same sound also has to register on three devices for a human to have access to the audio. If it checks out, the next step is for a human to review a few seconds of audio in an effort to check for things like fireworks or a car backfiring.

Klepper also noted that the humans who listen in are very busy and often bounce from one quick-hit sound to the next. Furthermore, the company does not store any audio it records past 72 hours, leaving a small window for times that police need to review the audio to determine sequence of firing or how many shots there were.

What it really comes down to for ShotSpotter, Klepper said, is being able to articulate its operating system and its mission. Some communities have an immediate distaste for the idea of an audio sensor being monitored at all. The company, however, has had 100 percent buy-in when it has a chance to articulate what it does, how it does it and why.
On the debut episode of Government Technology’s new podcast, GovTech360, we spoke to Seattle Chief Privacy Officer Ginger Armbruster (pictured at right). She’s spent the last couple years building the city’s privacy practice, establishing policies and working throughout the organization to ensure new digital services are introduced in a way that doesn’t jeopardize citizen data. Here are a few excerpts from that conversation, which offers some best practices for gov tech companies looking to engage with the government market. Find the full episode and subscribe to GovTech360 wherever you get your podcasts.

Q: Is there a way for cities to embrace smarter technologies while protecting citizen privacy?
I believe there is. And I think it starts with an acknowledgment that nothing is for free. So the trade-off about employing smart technology has to be weighed against what you do with all the information you’re collecting. We have to take into account that this isn’t just our world. It’s the public’s information we’re dealing with. So when I sit down with different departments, the very first part of the conversation is, what are we going to do with the data we’re collecting? What data do you need? Why do you need it?

Q: What do companies that want to work with government need to know?
We want those companies to have done is their homework around the privacy and data policies: What do you do with the data you collect? Because so many business models are built around collecting data and selling it — I’m going to use it in this other way while I provide the service to the city that they need. And that may be OK, but I need to be able to answer those questions about the data. So I would love companies to come in with a clear idea of their data collection practices and what they’re using the data for and their privacy policy. I also want companies to understand the legal landscape of the city and state that they’re in. We’ve had people come in who have no idea about our public records act and so they get really surprised when they find out that everything is public. Companies tend to go into the departments and get people sold on benefits and that’s great. I used to be a salesperson. That’s certainly what you want to do to generate the interest. But don’t wait too long to get involved with the compliance side of the house. Don’t wait too long before you talk to the privacy and security people. Don’t wait too long before you realize they’re going to be the ones who say, “Nah, it’s not going to happen until I’ve had a chance to review you.” There’s a lot of delay that can happen while someone’s trying to sell something, and that can be a real disappointment and a real tension. So get involved early with the legal side of the house. Make sure you’ve covered your bases on those compliance issues. — Noelle Knell

This interview has been edited for length and clarity.
4 Work closely with government clients

Sofa makes benches with sensors that local government can use to gauge pedestrian density. Sensors like these are a cornerstone of evolving smart city efforts across the country, in major cities from Chicago to Atlanta. Sofa alone has worked with more than 100 cities, using sensors to gauge, for example, how many people pass through a park on a given day, or how popular a public event series is in terms of attendance.

Putting sensors in an urban environment, however, can raise privacy concerns within the community. Sofa is aware of this, said Ed Krafcik, the company’s vice president of city development. With that in mind, they work closely with their public-sector partners to establish unique sets of privacy guidelines for the individual communities in which their products are deployed.

How closely? Well, their relationship with the Mayor’s Office of Tech and Innovation in New York City was so robust that when that massive jurisdiction developed its Internet of Things Guidelines in 2016, it used Sofa’s bench product as a case study to refine its own privacy guidelines. Krafcik described Sofa’s approach to privacy as co-creation, as a partnership with the public sector to make sure specialized needs or concerns in cities are handled properly.

As was the case with nearly every company interviewed for this piece, the gov tech market dictates that Sofa make protecting privacy a factor in all of the products it designs. Otherwise, the demand for them might not be there at all.

“At the end of the day,” Krafcik said, “if the public doesn’t trust what we’re doing — whether it’s us or another technology company — the sustainability of that product going to scale in a city becomes almost none.”

5 Anonymize all data

Zencity, meanwhile, is a slightly different sort of company from the others featured here. Its product doesn’t monitor people in a community but instead uses artificial intelligence to collect data points for government from internal sources like 311, as well as external sources like social media feeds and local news reports.

Zencity, meanwhile, is a slightly different sort of company from the others featured here. Its product doesn’t monitor people in a community but instead uses artificial intelligence to collect data points for government from internal sources like 311, as well as external sources like social media feeds and local news reports.

Zencity co-founder and CEO Eyal Feder-Levy said that its processes only collect data from sources that are publicly available anyway. Second, it anonymizes all the data its products collect in the interest of protecting privacy.

“Our goal is to show clients the trends that are happening,” Feder-Levy said. “It’s not important to know it’s this person or that person. We don’t even take that into our database.”

The third major privacy protection that Zencity puts in place is an algorithm aimed at removing any potentially identifying data, such as names or addresses or other incidentally added details. That really speaks to the guiding rule for not only Zencity but other gov tech companies as well: Focus on a specific use case while at the same time doing whatever it takes to avoid identifying specific individuals. Zencity, for example, wants to help local governments know what bus routes citizens think should be available anyway. Second, it anonymizes all the data its products collect in the interest of protecting privacy.

“Our goal is to show clients the trends that are happening,” Feder-Levy said. “It’s not important to know it’s this person or that person. We don’t even take that into our database.”

The third major privacy protection that Zencity puts in place is an algorithm aimed at removing any potentially identifying data, such as names or addresses or other incidentally added details. That really speaks to the guiding rule for not only Zencity but other gov tech companies as well: Focus on a specific use case while at the same time doing whatever it takes to avoid identifying specific individuals. Zencity, for example, wants to help local governments know what bus routes citizens think should be available anyway. Second, it anonymizes all the data its products collect in the interest of protecting privacy.

“Our goal is to show clients the trends that are happening,” Feder-Levy said. “It’s not important to know it’s this person or that person. We don’t even take that into our database.”

The third major privacy protection that Zencity puts in place is an algorithm aimed at removing any potentially identifying data, such as names or addresses or other incidentally added details. That really speaks to the guiding rule for not only Zencity but other gov tech companies as well: Focus on a specific use case while at the same time doing whatever it takes to avoid identifying specific individuals. Zencity, for example, wants to help local governments know what bus routes citizens think should be available anyway. Second, it anonymizes all the data its products collect in the interest of protecting privacy.

“Our goal is to show clients the trends that are happening,” Feder-Levy said. “It’s not important to know it’s this person or that person. We don’t even take that into our database.”

The third major privacy protection that Zencity puts in place is an algorithm aimed at removing any potentially identifying data, such as names or addresses or other incidentally added details. That really speaks to the guiding rule for not only Zencity but other gov tech companies as well: Focus on a specific use case while at the same time doing whatever it takes to avoid identifying specific individuals. Zencity, for example, wants to help local governments know what bus routes citizens think should be available anyway. Second, it anonymizes all the data its products collect in the interest of protecting privacy.
Are You Ready for 2020?

As security chiefs prepare for the next decade, the stakes may have changed, but the charge remains the same.

Back in 2012, I wrote an article for CSO magazine titled, CISO 2020: Will You Be Ready? The charge to global security leaders at that time was to move beyond a focus on daily breach headlines, scary cyberstories or other fear, uncertainty and doubt in the security industry and toward building trusted relationships with business executives with a foundation of personal and professional integrity.

Fast-forward seven years to the edge of a new decade, and a colleague recently challenged me with this question: Has anything really changed? But before I answer, I want you to think about your organization’s security efforts. What has worked well over the past few years? What mistakes were made? How has your team recovered?

Security Vision for the 2020s

Virtually everything is on the table as we enter a new decade that will be defined by global innovation and technology breakthroughs. Companies and governments worldwide are jockeying for position to define the new technology landscape. Hold on to your safety belts, because the number of technology and security initiatives will also soar as we head into 2020. What’s different now is that cybersecurity will be at the center of executive discussions.

Headline news stories over the past decade, from Facebook privacy blunders to the federal Office of Personnel Management data breach, have (belatedly) taught most CXOs that cybersecurity can’t just be bolted on at the end of production processes. Business leaders now recognize that earlier involvement of cybersecurity experts can help avoid a major data breach, which could derail innovative plans, cripple production operations, or worse, cause a total loss of trust in the brand or government organization. In order to build security into a new product or service, you need to know what the potential problems will be.

So what’s my advice?

1 / Do your homework. Research needs to be done internally regarding future business plans and externally with new technology and specific innovation alternatives available. Focus on secure alternative solutions. CISOs and other security leaders must engage now as businesses redefine themselves (again). Get involved in development life cycles. Security capabilities are a true enterprise priority.

Tip: The goal for security leaders is to be the trusted business partner who offers clear risk-based alternatives. Be known as an enabler of innovation with the right level of security deployed.

2 / Align business, IT and cyberpriorities. Andrew Haggard, a former PriceWaterhouseCoopers executive, said, “The biggest business and IT collaboration challenge faced by our clients is a lack of a clear alignment across business stakeholders and between business and IT teams of what capabilities are a true enterprise priority”

Tip: The goal for security leaders is to be the trusted business partner who offers clear risk-based alternatives. Be known as an enabler of innovation with the right level of security deployed.

3 / Lead the change. Cybersecurity can no longer be added at the end of project development life cycles. Security teams must be in the room regarding all strategic initiatives for the 2020s.

Tip: Look for cross-discipline opportunities. From smart cities to transportation projects to new data collected via Internet of Things devices, cybersecurity must be involved at every stage of the development and production processes. For example, rigorous testing, which includes global bug bounties, has become the new normal with next-generation vehicles. So does my article from 2012 still apply? With a few tweaks, yes. Although many things have changed in cybersecurity over the past seven years — including the higher stakes, the level of global attention and the global cybersecurity need to focus on trust, relationships and, most importantly, integrity remains.

Daniel J. Lohrmann is the chief security officer and chief strategist at Security Business magazine. He is a nationally recognized cybersecurity, leadership and author. From 2002 to 2014, and author. He is an internationally recognized cybersecurity expert and author. From 2002 to 2014, and author. He is an internationally recognized cybersecurity expert and author. From 2002 to 2014, and author. He is an internationally recognized cybersecurity expert and author. From 2002 to 2014, and author. He is an internationally recognized cybersecurity expert and author. From 2002 to 2014, and author.
Motoring

This summer, Bird, one of the big names in scooter shares, is set to roll out its newest micromobility offering: an electric motorcycle. The Bird Cruiser carries up to two adults and features hydraulic disc braking, a padded seat, a 52-volt battery, and pedals or pegs to rest your feet on. While it will initially only be available in select locations, the motorcycle has the potential to expand last-mile travel options for those with accessibility issues who cannot ride a scooter.

Source: Engadget

Moon Landing

It sounds like the stuff of sci-fi, but German scientists have developed a laser that turns moon dust into material that can be used to print 3-D objects. The device would solve two issues of lunar exploration: the cost of getting tools and materials to the moon and the annoyance and inconvenience of moon dust, which can clog machines and harm astronauts’ health. Called MOONRISE, the device weighs about six-and-a-half pounds and melts lunar dust down and forms it into new materials, primarily bricks that could be used to build structures. The goal is to have the tech ready for a 2021 German moon mission.

Source: Digital Trends

Send Spectrum ideas to Managing Editor Lauren Harrison, lharrison@govtech.com
Read full reports and breaking news about career changes across tech-driven roles in government at govtech.com/people.

Local CIO Departures in Nevada
After almost seven years with Henderson, Nev., CIO Laura Fucci announced her retirement in May, citing health concerns. She was previously CIO of Clark County, Nev., a position from which Michael Lane stepped down in May, having served in the role since December 2016. Before that, he was deputy CIO since August 2013. The county will conduct a nationwide search for a replacement.

New CIO in Genesee County, Mich., Following Cyberattack
Genesee County, Mich., hired Carl Wilson to head its Information Technology Department after previous CIO Chris Newell resigned following a ransomware attack in April. The department has since made strides to shore up its cybersecurity, and Wilson, who previously worked in nearby Oakland County, was part of a team that helped Genesee County recover from the attack.

Colorado Hires First-Ever Blockchain Architect
Gov. Jared Polis created the position of blockchain solution architect in Colorado, the first of its kind in the state. Thaddeus “Thad” Ball was appointed to serve in the role, which is part of the Governor’s Office of Information Technology. “The creation of this Blockchain Solution Architect role is breaking new ground and a step in the right direction to secure Colorado as a leader in blockchain innovation,” Polis said in a statement.

Michigan Launches Search for New IT Chief
Michigan has been without a CIO since David DeVries stepped down at the beginning of the year following the election of Gov. Gretchen Whitmer. In late May, the state announced its nationwide search to fill the position, which under the new administration will report to the governor and the director of the Department of Technology, Management and Budget, Tricia L. Foster.

Alex Alben Leaves Washington State
Washington Chief Privacy Officer Alex Alben, the first to hold the position since it was created in April 2015 by Gov. Jay Inslee, left the state in May. Alben was a winner of Government Technology’s Top 25 Doers, Dreamers and Drivers award in 2017. He was replaced by Will Saunders, who was previously senior program manager for Washington Technology Solutions’ open data team.
Fairfax County, Va., CTO Moves on After 20 Years

Wanda Gibson, head of IT in Fairfax County, Va., for two decades, announced a move to nearby Prince George’s County, Md., where she will serve as CIO. She was a Government Technology Top 25 Doer, Dreamer and Driver in 2010, among numerous other accomplishments. Gibson was recruited by Prince George’s County to take on a new customer relationship management project, the rollout of new ERP software and an update to the county website.
Staying Relevant by Getting Specific

Social media isn’t valuable to an audience if communications are too broad.

Recently received a quarterly email newsletter from my city government. It was visually appealing, well-written, and included over a dozen announcements about their accomplishments, services offered, and even more links to additional news and announcements.

What’s the problem? I clicked the print button and this email newsletter was the equivalent of six printed pages. Don’t get me wrong, the problem isn’t necessarily the length. The issue is that it’s six pages of information targeted to everyone, from people who are interested in local parks and sustainability to job seekers and business owners to you name it.

You can’t expect citizens to read a newsletter, watch a video or follow you on social media when they only expect to see something relevant to them a fraction of the time. They move on to something that speaks to them about what they care about.

You’re not relevant to your public when you’re not targeting their interests 99 percent of the time.

Running Services Like Mini-Brands

One answer might be setting up a communication strategy for each department or service like it’s a mini-brand that operates under a brand family (your government agency as a whole). As a business owner, I might want to interface with my local government on matters concerning commercial districts and sales taxes. For someone like me, a business-focused email newsletter and related Facebook page would be highly relevant.

Topic-specific email lists are nothing new for government, but it’s not good enough to place all your citizens in a catch-all list and only show them your interest-specific options as a last resort when they click the “unsubscribe” button.

Perhaps it’s time to relax my long-standing advice to government with regard to centralized social media profiles. Many times, when departments, divisions or agencies want to run their own pages, we urge them to contribute instead to the primary agency profiles. We cite supporting reasons like resources needed to maintain profiles and the small audiences that those profiles inevitably earn.

However, a mere 450-person Facebook audience for a highly specialized topic is not a waste of time and effort if those people are highly engaged with their government on a topic that matters to them.

Kristy is known as “GovGirl” in the government technology industry. A former city government Web manager with a passion for social media technology and the lighter side of government life, Kristy is the CEO of Government Social Media.
CONGRATS
2019 Special Districts Technology Innovation Award Winners!

WEST REGION

Citizens Category
Moulton Niguel Water District
MyWater MNWD

South Coast Air Quality Management District
Mobile App

Southern Nevada Health District
Food Handler Card Testing System

Operations Category
Greater Los Angeles County Vector Control District
Mobile App and Supporting Infrastructure

Menlo Park Fire Protection District
Mobile Special Technology & Aerial Response (MSTAR) Concept Vehicle

Metropolitan Water District of Southern California
Real-Time Distribution System Monitoring Using Mobile Technology and myEBS Search

Leadership Category
Midpeninsula Regional Open Space District
Stefan Jaskulak, CFO/Director of Administrative Services

SunLine Transit Agency
Lauren Silver, CEO/General Manager

South Coast Air Quality Management District
Ron Moskowitz, Chief Information Officer

NORTHEAST REGION

Citizens Category
Norwalk Transit District
Wheels2U Micro-Transit Service

Philadelphia Parking Authority
meterUP Mobile Pay App

Operations Category
Pittsburgh Water and Sewer Authority
Web-based Applications

Leadership Category
Port Authority of New York and New Jersey
Margaret Zampini, Manager, IT Communications and Customer Services

Public Parking Authority of Pittsburgh
Philip True Savino, Chief Technology Officer

Port Authority of New York and New Jersey
Ai Yamashita, Data Analytics Program Manager, Aviation Department

To learn more about the winners’ initiatives and the Special Districts Program, visit: govtech.com/districts
YOU'RE REQUIRED TO KEEP RECORDS FOR UP TO 10 YEARS.

BUT DON’T WORRY. WE GOT YOUR BACK.
Preparing for the Network of Tomorrow, Today

A government executive’s guide to understanding the network of the future and its role in transformative change.
In Dallas, intelligent sensors will detect when a street light is out and automatically alert repair crews. In the San Francisco Bay Area, officials will use video analytics from traffic cameras to monitor congestion and automatically adjust express lane tolls. And in Georgia, virtualization and other new technologies will enable the state’s central IT organization to roll out new capabilities faster than ever before to support the needs of state agencies.

It’s clear that state and local governments are in the midst of a technology revolution. Cloud models, “as-a-service” solutions, Internet of Things (IoT), artificial intelligence (AI), mobile devices and other innovations are already helping public sector organizations improve services to constituents; save money, time and labor; and keep workers happier and more productive.

But fundamental to these advancements is network connectivity on an unprecedented scale. As states and cities grow smarter and more connected, enterprise networks will need to be more scalable, available, accessible and secure than ever before — even as architectures, devices and applications continually evolve.

This is tough to do, however, when capital-intensive networks are reaching end of life and are difficult to maintain. According to a NASCIO survey, 90 percent of state government agencies say at least one-fifth of their IT infrastructure is a legacy system. It’s a risky way to operate.

"[Government agencies] used to be able to buy equipment for their networks, and as long as it still received power they could use it for a long time with the intent of using scarce government dollars as efficiently as possible,” says George Spencer, associate vice president, AT&T Public Sector. “Over time, it’s harder to maintain this equipment, so they fall behind.”

Old network strategies simply won’t work in an environment where new technologies emerge at an exponential pace, user expectations change rapidly and security threats continually multiply — all while state and local budgets remain stagnant.

It’s time for forward-thinking government leaders to embrace a new approach. We call it the network of tomorrow. This guide will show you what it is, and how you can get there.
The Network of Tomorrow

The network of tomorrow is characterized as much by the technology that underpins it as the innovation it enables. While yesterday’s network was based on capital-intensive hardware implementations, the network of tomorrow is software-based, enabling organizations to flexibly set up, change and secure network environments without purchasing and deploying expensive physical devices. Instead, features and capacity can be changed via software configuration. And intelligent automation within the network enables it to deliver a level of performance and reliability that is crucial in an everything-is-connected world.

“IT’s really about an intelligent network,” says Greg Kaleski, product marketing manager, AT&T Public Sector. “The WAN is no longer a static, one-size-fits-all thing, because you can now control the route that different apps can take, you can have one vendor bringing in a wireline connection and another vendor bringing in a mobility connection and then route preferentially based on your needs.”

The result of these capabilities is a network that quickly scales up capacity when it’s needed and scales back down when it’s not. This software-centric, cloud-based approach also alleviates staffing and resource burdens associated with in-house network deployment. Agencies can add applications to the network without waiting for the IT team to build out more bandwidth; therefore, new services roll out remarkably fast. Just as important, sophisticated security features are built in and maintained by top industry talent.

“Software-defined networking enables a new model and that’s significant. We aren’t just evolving; we are looking at a paradigm shift for how governments provide service to their end users,” says Michael Keenan, technical sales manager, AT&T Public Sector. “We’re moving from a model where you’re locked in with different vendors and buying a whole bunch of boxes that you have to support to an approach where you are subscribing to a service and paying a rate for what you use.”

Network Functions Virtualization (NFV)

This replaces dedicated routers, firewalls and other traditional network hardware with software that runs on commercial servers and performs these functions through an application instead of hardware.

Network as a Service (NaaS)

This is a model for consuming network services virtually on a pay-for-use basis or for a monthly fee. The service provider is responsible for network operations and management.
The Georgia Technology Authority (GTA) is the central IT authority for the state of Georgia. In collaboration with AT&T, it’s using a managed services approach to deliver wide area network (WAN), local area network (LAN), voice and other network services to the 1,300 state and local government entities that it serves. A third-party integrator handles the day-to-day coordination and management of service delivery. When end users need new network capacity, changes or repairs, they simply put in a request for service.

“Managed services save the state a lot of time, effort and resources; the network is secure, reliable and recoverable; and there’s a built-in refresh cycle so technology is always up to date,” says Dean Johnson, Chief Operating Officer of GTA.

The solution has also alleviated the need for a large staff of skilled network technicians because qualified service providers handle day-to-day technical tasks. As part of its collaboration with AT&T, GTA plans to implement SDN and more virtualization within the next few years. SDN is essential for Georgia to meet its growing IT demands, including delivery goals that GTA established in a new contract for server services. GTA needs to enable faster network provisioning so that it will align to the rapid provision capabilities the service provider plans to implement.

“We’re committed to the goal of being able to deliver a standard, virtual or cloud server within one day,” says Johnson. “These aggressive timelines are light years from where we are today, and they would be very difficult to meet without introducing more automation and some prepackaged functionality — such as pre-assigned IP addresses, VLANs and firewall configurations — that we’re currently working with AT&T to architect and engineer.”

“We’re committed to the goal of being able to deliver a standard, virtual or cloud server within one day.”

- Dean Johnson, Chief Operating Officer, GTA
Future Ready

The network of tomorrow helps state and local organizations prepare for many current and future challenges and trends, such as cybersecurity, mobility, IoT and other innovations.
Enhancing Cybersecurity

According to NASCIO, security and risk management has been the No. 1 priority of state CIOs for the last five years. But recruiting and retaining qualified IT and cybersecurity staff is a huge challenge for state and local governments, who are losing expertise and institutional knowledge at the same time they must compete with the private sector for skilled IT and cybersecurity personnel.

"Many state and local governments struggle to acquire and maintain the resources required to gather intelligence and protect themselves, their constituents and their critical infrastructure from digital attacks," says Princess Young, a cybersecurity awareness program lead for the Department of Homeland Security.

And although cybersecurity is a top priority in most organizations, the approaches many of them take to prevent breaches are antiquated. "The prevailing methodology in cybersecurity right now is the defense-in-depth approach, where organizations put hardware appliances in place to do specific security functions," says DuWayne Aikins, principal architect, AT&T Public Sector. "But that's costly and time consuming and by the time those solutions are installed they need to be refreshed. They simply can't keep up with the rapidly evolving threat landscape or today's extensive network ecosystems."

Today's attacks are often stealthy, targeted and persistent; range from ransomware and distributed denial of service (DDoS) attacks to encrypted malicious web traffic and phishing attacks; and exploit vulnerabilities in cloud services, mobile applications, the IoT and other resources. Emerging technologies and the movement of data to and from off-premises locations further expose the network to vulnerabilities and risks. Traditional security hardware such as firewalls, routers and intrusion prevention systems cannot protect data once it leaves the enterprise, and it is inadequate against threats that use encryption or other legitimate resources to make it past ordinary lines of defense.

The modern threat environment requires a shift in focus to intelligence gathering, incident detection and rapid remediation. The network of tomorrow allows states and local governments to easily incorporate these functions via virtualization and managed services. In addition, the network of tomorrow is easier to set up and provision than a traditional network, which means IT and cybersecurity teams can quickly adjust configurations to reduce risks and remediate threats. "When functions are centralized and virtualized, it's a lot easier to have a unified security posture," says Aikins. "The use of software and virtualization is vital for both current and aspiring cybersecurity professionals to face the unique challenges that this field presents," adds Young. "These technologies are particularly powerful when combined with other resources and research, including everything from educational programs to other risk management solutions."

Looking into the future of network security, Don Parente, associate vice president of engineering and architecture, AT&T Public Sector, foresees the increased use of SDN for network compartmentalization. Many government intranets have thousands of public sector employees on them. With such ubiquitous access, the insider threat and the risk of unauthorized access increase. "With SDN, we can quickly set up purpose-built networks with very few people on them. If you can define a network in near-real-time and reduce authorized communities to smaller groups, then you can contain information more easily," says Parente.

"When functions are centralized and virtualized, it’s a lot easier to have a unified security posture.”

- DuWayne Aikins, Principal Architect, AT&T Public Sector

Industry experts agree that open information sharing within an organization and with technology vendors is vital to maintaining a robust security posture. George Spencer, associate vice president, AT&T Public Sector, says that many CISOs and their organizations make the mistake of going at it alone and think their team and security controls are sufficient to fully protect their environment.

“‘It takes an army to successfully win the battle on an ongoing basis,’ he says.

Spencer recommends organizations engage in public-private partnerships and keep the lines of communication open.

Young agrees: “Collaboration across all sectors is increasingly vital to the security of organizations and individuals across the nation. Sharing threat indicators, potential risks, observed trends and new technologies allows us to build resilience against cyber threats.”

Tips for Success: Engagement and Communication are Key

Industry experts agree that open information sharing within an organization and with technology vendors is vital to maintaining a robust security posture. George Spencer, associate vice president, AT&T Public Sector, says that many CISOs and their organizations make the mistake of going at it alone and think their team and security controls are sufficient to fully protect their environment.

“‘It takes an army to successfully win the battle on an ongoing basis,’ he says.

Spencer recommends organizations engage in public-private partnerships and keep the lines of communication open.

Young agrees: “Collaboration across all sectors is increasingly vital to the security of organizations and individuals across the nation. Sharing threat indicators, potential risks, observed trends and new technologies allows us to build resilience against cyber threats.”
CASE STUDY

The use of shared services is a main tenet of Michigan’s Oakland County Department of Information and Technology. Recognizing that not all departments and agencies have the IT expertise and resources to do everything on their own, the county uses a model where the larger organization shares services with smaller ones. One example is its G2G Cloud Solution, which provides e-commerce capabilities to counties throughout the state and is supported by network services from AT&T.

“We’ve found that by sharing, smaller governments don’t need to buy and we can lower our overall cost of transactions,” says Phil Bertolini, CIO for Oakland County.

Security is woven into shared services. This approach takes the burden off smaller departments and helps ensure they are protected. Ultimately, it also protects the network as a whole.

“Without the network, none of this happens. The cloud, IoT and other innovations don’t work without connectivity,” says Bertolini.

To that end, the county is in the middle of a complete modernization of its networks. SDN and virtualization are key aspects of the overhaul and will enhance the department’s ability to quickly secure and manage traffic across these networks.

“With virtualized security functions, greater visibility and automated controls, we can add capacity and take advantage of new opportunities much faster,” Bertolini says.

“With virtualized security functions, greater visibility and automated controls, we can add capacity and take advantage of new opportunities much faster, at far lower cost and with more consistent security policies across the network,” Bertolini says.
State and local agencies need to provide ubiquitous, on-demand network access to multiple groups of users, including a new generation of remote workers and a diverse constituency. Governments are trying to support a workforce that increasingly includes employees who want to log in from home or a local café. They are also trying to accommodate remote work to alleviate the high cost of office space and improve productivity and workflows for people in the field,” says Keenan. At the same time, citizens, businesses and private partners expect 24/7 access to personalized, consumer-like mobile services, as well as smart city innovations that improve quality of life, save taxpayer dollars and spur economic growth. This demand for a more mobile-friendly government not only increases WAN traffic and bandwidth requirements, but also introduces new routing challenges as thousands of devices at the edge attempt to access network resources and cloud-based services. Smart devices, which are now the computing device of choice for many users, strain the network even further and create unpredictable demand by streaming video, using VoIP and performing other data-intensive processes. Traditional hardware-based network approaches cannot scale as quickly and flexibly as needed to meet this demand. They cost too much, take too long to deploy and rely on human intervention.

The network of tomorrow provides flexible, software-based network services that, in essence, can run themselves. By allowing the network to automatically create virtual network connections, these services can provide processing power and new routes on demand. Organizations can accommodate citizen, workforce and line-of-business demands for secure, reliable, high-performance mobile connectivity within days — if not hours. Using SDN and virtualization, for example, agencies can automatically provision additional capacity in the event of a disaster; use quality of service (QoS) prioritization to ensure critical applications are continuously available to mobile users; differentiate routing so highly sensitive mobile communications travel a different, more secure route than other types of data; and optimize routing to make the best use of existing resources.

Tips for Success: Plan for the Non-Wired WAN

In the near future, schools and some government agencies won’t have wired connections anymore because their networks will be based on 5G or 6G cellular connections. As this evolution continues, organizations that support WAN will have to consider non-wireline solutions and their strategy to implement them. “With WAN, you have to start thinking about mobile data connections, because whether they’re supportive, backup or — with the advent of 5G — primary WAN connections, you’re now moving away from a purely wireline model to these new technologies,” says Spencer.
The Contra Costa Transportation Authority (CCTA) in California’s Bay Area is working on several projects that rely on mobile connectivity to improve transportation across the region. One project is to relieve heavy congestion along Interstate 680. The project will rely on video cameras to monitor traffic speeds, and then use that data to automatically set tolls for express lanes. In addition, when traffic drops below a certain speed, buses will be able to use the right shoulder, and ramp meters will hold traffic on nearby onramps until a bus passes by. All of this will be coordinated via the wireless network.

When asked what organizations should consider when undertaking similar projects, Randy Iwasaki, Executive Director of CCTA, emphasizes the importance of network reliability and flexible bandwidth.

“Network safety from both the transportation and mobile connectivity perspective is going to be increasingly important,” Iwasaki says. “You’re going to get a lot more data from cell phones in the future and you need a network that can handle that. You have to have a redundant system to ensure network communication is never lost, and you need expandable bandwidth for quickly relaying high volumes of video and other data back and forth.”

“You’re going to get a lot more data from cell phones in the future and you need a network that can handle that.”

- Randy Iwasaki, Executive Director, CCTA
When it comes to IoT security, AT&T advocates for an "Intra
net of Things" rather than a public internet of things. An Intranet
of Things is an internal network with private IP addresses. With
a next-generation network, organizations can easily set up an
intra
et for a specific purpose. “People are one of the main
causes of breaches — whether they mistakenly click on a malicious email or intentionally
do harm. With the flexibility of an advanced, software-based
network, you can mitigate that threat by separating networks for things from networks for people,” says Parente. “The
network is already there. It’s just a simple matter of provisioning.”

States and cities are adopting IoT technologies to do everything from manage
energy efficiency in public buildings to monitor flood levels. While IoT brings new levels of efficiency, cost savings and innovation to state and local governments, it also creates new complexities. IoT not only increases the amount of data traveling across the network, but also the number of endpoints — potentially hundreds of thousands — connecting to the network. In addition, each device and use case has unique requirements for power, bandwidth, reliability and communication with other applications or devices. These requirements impact the type of network technology IoT requires (e.g., Bluetooth, Wi-Fi, 4G, or Ethernet/LAN); depending on the use case, organizations may need to create multiple network connections.

IoT security is also a challenge. Besides concerns about device vulnerabilities, organizations must be sure the network itself and data connected to devices is protected. Next-generation networks give organizations the tools they need to flexibly set up, customize and secure IoT networks. SDN allows them to centrally manage data flows on highly distributed IoT networks; NFV allows them to virtually provide the unique combination of functions that each IoT use case requires; and NaaS allows them to quickly add bandwidth as needed. For example, an organization can partition part of the network infrastructure to provide a virtual dedicated space for a specific application.

Tips for Success: Implement an Intranet of Things

When it comes to IoT security, AT&T advocates for an "Intranet of Things" rather than a public internet of things. An Intranet of Things is an internal network with private IP addresses. With a next-generation network, organizations can easily set up an intranet for a specific purpose.

“People are one of the main causes of breaches — whether because they mistakenly click on a malicious email or intentionally do harm. With the flexibility of an advanced, software-based network, you can mitigate that threat by separating networks for things from networks for people,” says Parente. “The network is already there. It’s just a simple matter of provisioning.”

"You can mitigate that (human) threat by separating networks for things from networks for people."

- Don Parente, Associate Vice President of Engineering and Architecture, AT&T Public Sector
With a video camera and AI system, we can dispatch crews when the park needs attention.”

- Michael Sherwood, Director of Innovation and Technology, Las Vegas
The fifth generation of mobile networks, 5G, will ultimately revolutionize the way government entities operate and serve citizens. In December 2018, AT&T became the first and only company in the U.S. to offer a mobile 5G network. 5G and edge computing have the capacity to deliver an unprecedented opportunity to augment and elevate the human experience.

Edge computing can shift the workload of transmitting vast amounts of data away from hardware to the network, through software-defined applications. This model allows businesses to route applications’ specific traffic to where they need it and where it’s most effective, whether that’s in the cloud, the edge of our network or on their premises. Today’s applications are high-performance and power hungry, generating massive amounts of data that require real-time computing power.

“Edge computing helps fulfill the promise of the cloud to transcend the physical constraints of our mobile devices,” says Andre Fuetsch, president of AT&T Labs and chief technology officer, AT&T Communications. “The capabilities of tomorrow’s 5G are the missing link that will make edge computing possible.”

Mobile 5G will be about more than just speed. It will also eventually bring ultra-low latency — a key enabler for virtual reality, autonomous vehicles and IoT, all of which depend on a highly efficient network response to orchestrate.
Meeting the security challenge for 5G mobile networks is a key focus for service providers, manufacturers and other stakeholders. Some believe moving computing power and other capabilities closer to the edge inherently makes networks less secure. However, technologies such as network virtualization and edge computing together with device management and automated threat detection and response will help create more flexible and highly secure networks to meet this challenge. Software-defined networking makes it possible to develop a multilayered approach to security that simultaneously considers the communication layer, hardware layer and cloud security. Government operations stand ready to benefit from sophisticated access management capabilities while increasing their security against distributed attacks by cyber threats.

In addition, AT&T is working to enable an ecosystem of 5G devices, all connected to an intelligent, software-driven network that can react in near real-time. With these capabilities, ideas that seemed like science fiction will increasingly start to become reality. Tomorrow’s robots will be deep learners, harnessing edge computing to process massive amounts of data in order to get smarter as they go about their business. The successful progression of 5G networks will deepen the human-machine relationship.

AI and human “hybrid intelligence” combines human knowledge, flexibility, beliefs, and instincts along with the blindingly fast speed and steadiness of machine logic.

“Robots will learn from their mistakes and share what they learn collectively so all of the robots improve over time,” says Ken Goldberg, UC Berkeley Professor of Robotics, Automation and New Media. Instead of fearing a robot revolution, we can look forward someday to working alongside intelligent machines designed to help us successfully achieve our goals.

In addition, 5G will eventually support an explosion of immersive experiences as mixed reality and digital twins expand our reach. Digital twins are real-time digital models of our cities, factories and other environs that could enable predictive, crystal ball-like simulations. As populations continue to grow, city planners are constantly challenged with the impacts to traffic patterns, pedestrians, video surveillance, real estate and more. Over the next decade, the network will become an overlay on top of our physical world. Virtually every object, every interaction and every observation will become a piece of data which informs advanced simulations. The use cases across the public sector seem limitless.

Test use cases with industry leaders on AT&T’s live mobile 5G network. The goal is to bring future 5G experiences to life today.

“Robots will learn from their mistakes and share what they learn collectively so all of the robots improve over time,” says Ken Goldberg, UC Berkeley Professor of Robotics, Automation and New Media. Instead of fearing a robot revolution, we can look forward someday to working alongside intelligent machines designed to help us successfully achieve our goals.

In addition, 5G will eventually support an explosion of immersive experiences as mixed reality and digital twins expand our reach. Digital twins are real-time digital models of our cities, factories and other environs that could enable predictive, crystal ball-like simulations. As populations continue to grow, city planners are constantly challenged with the impacts to traffic patterns, pedestrians, video surveillance, real estate and more. Over the next decade, the network will become an overlay on top of our physical world. Virtually every object, every interaction and every observation will become a piece of data which informs advanced simulations. The use cases across the public sector seem limitless.

5G’s ultra-fast speeds and ultra-low latency will ultimately help enable a convincing virtual world for learners to collaborate as never before. Recess could become in-the-field research by superimposing a digital understanding of physics on playground equipment. Imagine high school students thousands of miles away controlling a robot inside an active volcano. And graduate students across the world exploring the rain forest together and virtually discussing their findings. Each of these learning experiences will be social, connected, collaborative and immersive — driving deep engagement and elevating the human experience.

The AT&T 5G Innovation Program, launched in February 2019, will develop ideas and test use cases with industry leaders on AT&T’s live mobile 5G network. The goal is to bring future 5G experiences to life today.

“Robots will learn from their mistakes and share what they learn collectively so all of the robots improve over time,” says Ken Goldberg, UC Berkeley Professor of Robotics, Automation and New Media. Instead of fearing a robot revolution, we can look forward someday to working alongside intelligent machines designed to help us successfully achieve our goals.

5G will be about more than just speed. It will also eventually bring ultra-low latency — a key enabler for virtual reality, autonomous vehicles and IoT.
Industry experts recommend the following suggestions to better understand, design and activate the network of tomorrow.

**UNDERSTAND**

Identify stakeholders' needs.
The Georgia Technology Authority (GTA) invites executive branch agencies to actively participate in defining business and technical requirements and evaluating proposed solutions. “Doing so helps ensure that service providers meet individual agencies’ needs in addition to the needs of the enterprise, and helps to ensure buy-in throughout the life of the relationship,” says Johnson of GTA.

Understand the current landscape and environment.
Document what is on your network or what connects to your network (e.g., data, applications, mobile devices, SaaS applications, IoT sensors) and standardize approaches and allows you to negotiate the best rates and contracts.

Update network procurement practices and policies.
Be sure RFPs and other processes can accommodate new service models, such as NaaS. Where possible, take advantage of other organizations’ contract vehicles to streamline procurement.

Formalize processes.
Doing so ensures network capacity and security requirements are always considered (and budgeted for) when new services are added or infrastructure changes are made.

Pick your vendors wisely.
Choose a stable, experienced vendor that has a history of success and a culture of innovation.

**DESIGN**

Develop a plan.
Clarify business goals and map those goals to the appropriate technology. Consult with the vendor community to understand what’s possible and determine a roadmap for getting there.

“Organizations usually need help to understand and segment their scope of work into areas. They have to take into account applications, resources, budget, procurement vehicles and more. It’s not just about technology. It’s about what happens on Day 2 and how you operationalize it and take care of it,” says Samantha Thibault, director of emerging technologies, AT&T Public Sector.

Prioritize.
Don’t wait to resolve every issue before getting started. Determine what you can do most quickly, look for quick wins and break projects into smaller, iterative pieces. “Doing things with software is much faster than doing things with hardware. You can instantiate new network functions virtually, simply by logging into a portal,” says Keenan.

SDN and virtualization also allow organizations to develop and test disruptive technology more quickly and iteratively, which allows them to fail faster. “Failure is a part of innovation, and it’s better to fail early than at a large scale,” Keenan says.

Incorporate all anticipated work into a single plan.
A master plan facilitates project management, helps standardize approaches and allows you to negotiate the best rates and contracts.

Update network procurement practices and policies.
Be sure RFPs and other processes can accommodate new service models, such as NaaS. Where possible, take advantage of other organizations’ contract vehicles to streamline procurement.

**ACTIVATE**

Educate.
Be sure procurement staff and legislative bodies understand the unique characteristics and requirements of a next-generation network. Provide IT personnel ongoing training in managing services and performing other tasks that are not traditionally within their purview.

Communicate.
Share information and solicit input internally, across departments and agencies, and with vendors to encourage adoption and stay current on opportunities and risks.

Regardless of where government organizations stand on the road to the network of tomorrow, it’s time to move forward. The opportunities are waiting, and the future is now.
Our first name has always been American, but today you know us as AT&T. We’re investing billions into the economy, providing quality jobs to over 200,000 people in the U.S. alone. We’re supporting the veterans who make our country stronger and providing disaster relief support to those who need it the most. By bringing together solutions that help protect, serve and connect — committed AT&T professionals are working with the public sector to transform the business of government. No company is more invested in America’s future than AT&T.

att.com/publicsector

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation’s only media and research company focused exclusively on state and local government and education.

govtech.com