ANNIKA HAAS/FLICKR (CC BY 2.0)

Estonia allows its citizens to go online to perform almost every interaction they have with government.

PUBLIC SERVICES

Digital citizens

Electronic-government initiatives could help states to run more smoothly, but they raise serious security questions.

BY NEIL SAVAGE

The offices of the Massachusetts Registry of Motor Vehicles were filled with angry, frustrated people, waiting in lines for up to five hours to renew their driving licences. It was March 2018, and the registry had just installed new software and brought in tougher identification requirements to comply with the Real ID Act, a federal law that was intended to improve the authenticity and security of the licences.

Applicants were required to bring to the office a selection of paper documents to prove their identity and residency status: a social security card or tax document, a validated birth certificate, a passport or immigration papers, a recent utility bill and a bank statement. But staff were struggling to use the new software. Checking that everyone had all the right papers, and then getting the system to produce a new licence, was taking much longer than expected. The problem continued for several weeks — and was happening in other US states, too.

Long queues, flawed data and problems dealing with paper documents are exactly the sorts of issue that digital government is supposed to avoid. Proponents argue that in this digitized age, dealing with the state should be as easy as buying socks online. Digital government, sometimes called electronic government (e-government), should provide a painless way to navigate bureaucracy, to make state services operate more efficiently, and to save money. It should also make government more transparent, giving citizens more access to government data and providing more insight into, and better control of, the state's activities. Applying artificial intelligence to government data could help to fight crime and terrorism, improve economic decision-making, and cut the costs of doing business internationally.

Some of that promise is being fulfilled in certain countries. But there are issues still to be worked out concerning how to transform government operations, keep personal data private, and make the best use of emerging information technologies.

"People's expectations for government services are the same as they have of all other digital interactions in their daily lives," says Steve Hurst, who heads Deloitte Consulting's Digital Government group in New York. "If you don't meet those expectations, it affects people's perception of the quality of government."

Estonia is often held up as a model of how to do e-government well. Citizens can file their tax returns, vote in elections and register a birth or a new company online. Almost anything except buying a house or getting married can be done from anywhere with an Internet connection. An encrypted state ID enables access to everything from government websites to bank accounts. The country has introduced electronic residency, allowing people anywhere in the world — for a fee — to obtain an ID, register a business in Estonia and sign documents, boosting the country's commercial sector. More than 46,000 people have become virtual Estonians in this way — equivalent to around 3% of the country's physical population.

Other countries are also pushing ahead with digital services. According to the United Nations Department of Economic and Social Affairs, in 2018, Denmark was best at using Internet technologies to deliver public services, followed by Australia, South Korea and the United Kingdom. The United States ranked eleventh, just behind Japan. The nations with the least capacity were predominantly those African countries that lack widespread Internet access and even the electricity to make e-government feasible.

Digitizing government is about more than easing the pain of citizens who encounter bureaucracy. It is also intended to cut costs by making the provision of government services more efficient. The UK Treasury has estimated that implementing the website www.gov.uk, which launched in 2012 and merged the websites of all 25 ministerial departments and 385 other public agencies into a single portal, saved taxpayers £3.6 billion (US$4.7 billion) in its first three years of operation.

The power of digital government lies in making all the data that governments collect and generate, such as crime rates and spending on education, available to both government officials and the public. In this way, citizens can not only find useful information, but also gain insight into how the state is working.

Citizens should be able find anything they want to know online, says Rodrigo Sandoval-Almazán, a political scientist at the Autonomous University of the State of Mexico in Toluca, who is working with the Mexican government to develop regulations for digital services. Mexican law requires officials to provide answers to the public's questions, but he would prefer citizens to be able to get the answers they need straight from databases, rather than waiting for an official to produce a report. "If I have a question about the expenses of public schools in my area, or what the best schools for my kids are," he says, "the technology should give me the correct answer."

INTELLIGENT SOLUTIONS

The state can benefit from applying artificial intelligence to its data, says Jaideep Vaidya, a computer scientist at Rutgers Business School in Newark, New Jersey. He is developing

RENEE ALTROV/ENTERPRISE ESTONIA

data-analysis software for Newark that will help to make decisions on the basis of citizen complaints. Residents tweet about the presence of potholes or broken streetlights, and an algorithm collates and summarizes the information, and suggests the most efficient way to deal with the problem. For instance, it might provide an optimized route that allows a road crew to fix the largest number of potholes in the shortest possible time, rather than sending trucks out randomly when complaints come in. Algorithms that suggest routing strategies for supplies and emergency services could also be useful after a hurricane or earthquake, and have the potential to save a lot of lives.

Newark — a densely populated city with a poverty rate of almost 30% — has a large number of vacant plots, which do not generate property tax and sometimes attract crime. Vaidya says that predictive analytics can make computer models of different actions or incentives that might entice businesses to take over those plots. Officials can also use predictive analytics to work out the best way to bring in revenue, "which in turn lets you lower the tax burden", he says.

Applying predictive analytics to government data could help police departments to work out how best to allocate their resources. It might also help to detect terrorist plots or other security threats. But relying on artificial intelligence to make official decisions without critical oversight can cause problems, Vaidya warns. For instance, a machine-learning algorithm might build a model that relies on characteristics that are subject to antidiscrimination laws such as race or age, causing unfairness. Or it might use less-obvious proxies for race such as postcodes or the presence of certain businesses in an area.

"The problem is more complicated than just keeping the records internal."

"Everyone now is crazy about deep learning," Vaidya says, a technique that runs through many layers of mathematical calculations to mimic the way that the brain works. Among other accomplishments, it has allowed digital assistants such as Apple's Siri and Amazon's Alexa to perform reliable voice recognition, but it is not obvious even to the computer programmers how it comes up with a particular answer. "The big problem with deep learning is that you don't have an explainable model, so you basically can't understand why the algorithm is making particular choices," he adds.

TEMPTING SITES

One problem with putting information about taxes, employment and health-care access into one easy-to-access site is that the site becomes a target for hackers. "It essentially creates a honeypot," says Andrew Greenway, a partner at Public Digital, a UK consultancy that helps governments to design digital systems. "You know if you hack into that there's an enormous prize."

In 2017, e-government champion Estonia had to issue software updates for hundreds of thousands of ID cards after security researchers discovered a flaw in the cards' chip that left it vulnerable to hackers. The country's combined police and border force, which is responsible for issuing identity documents, released a statement at the time saying that they did not expect this to be the last security risk that the system will face.

Greenway, who was part of the team that set up www.gov.uk, says that government systems should segregate information, so that a hacker will have difficulty linking one piece of data about someone to another. But even if government databases remove names to obscure identity, comparing those databases to marketing lists or a telephone directory could allow some of those names to be recovered, says Eugene Spafford, a computer scientist at Purdue University in West Lafayette, Indiana. Additionally, a main component of digital government is providing citizens with easy access to their own information. "That's kind of the opposite, in a way, of trying to maintain security and privacy," Spafford says. "So the problem is more complicated than just keeping the records internal."

Computer scientists are now developing cryptographic techniques to keep data secure. One approach, which is growing in popularity because it enables data to be accessed but still protects identity, is called differential privacy. This allows a person to query a collection of records, but not to tell the difference between individual records. For example, someone could find out how many people claim a particular benefit, but not which people they are. Essentially, the computer calculates an answer, and then adds some statistical noise to obscure the source. However, it only works when numerous records are aggregated together, and it reduces the accuracy of the result. "It doesn't work everywhere, but it is extremely useful," Vaidya says. The US Census Bureau plans to use differential privacy to protect the data it collects in the 2020 Census.

THE OLD WAYS

Some of the problems with implementing digital government have little to do with technological developments. Instead, work is hampered by cost, outdated equipment, entrenched bureaucracy and a lack of political will. For instance, many digital systems still rely on archaic computer languages such as COBOL, which was created in 1959. "Some of the databases that a lot of tax systems are based on around the world are crumbling bits of COBOL that have been there for 40 years," says Greenway. "They're sort of stuck together with sticking plasters, but now they represent critical national infrastructure."

According to Spafford, some US agencies are using computers that are up to 30 years old. In 2015, the US Office of Personnel Management suffered data breaches that revealed the records of 4.2 million federal employees, as well as the social security numbers of 21.5 million people who had undergone background checks for security reasons. The breach showed that the office's systems used out-of-date hardware and software with vulnerabilities that current equipment would not have. "The cost to fix it was in the many millions of dollars," he says.

Estonia's ID cards contain chips that identify the user online — but that can pose a security risk.

Government employees are often reluctant to change the way that they operate — sometimes because laws and regulations spell out requirements for how to handle information, but also simply because of a lack of political will to change. "If they have the information, they have the power that provides," Sandoval-Almazán says. "Many senior public managers don't want to lose their power, and they see the technology like a threat." Corruption can also be a problem in some places, he points out. A well-functioning e-government is not compatible with a system that thrives on bribery and personal connections.

Implementing systems is not simply a case of adapting the technology to fit the work of government. It also entails transforming government to better fit the technological nature of the twenty-first century. Government departments need to be less compartmentalized and more willing to adapt, Greenway says, and should focus more on what citizens need. In that way, e-government is not just about creating a better customer-service experience for encounters with the state. "It's about reforming the bureaucracy and the institutions, and changing some quite fundamental behaviour in the civil services," he says. Digital technology has the potential to transform the way citizens deal with government, but it could also alter the way government sees itself. ■

Neil Savage *is a freelance writer in Lowell, Massachusetts.*