KPMG

@gov

Inspiring innovative government

Transforming government in the age of technology

kpmg.com/atgov

#atgov

Fall-Winter 2016

Contents

About @gov

@gov is a new digital magazine designed to deliver forward thinking and transformative insights to government professionals as they face increasing demands and emerging societal needs in a changing world.

Delivering in-depth insights spanning issues that affect both national and local governments, *@gov* looks at topics critical to success for governments today.

This printable digest contains a sample of the content you will find on kpmg.com/atgov.

For the latest *@gov* content subscribe to our mailing list by emailing government@kpmg.com.

From the editor

Welcome to the inaugural edition of *@gov*, the new digital magazine from KPMG, designed for government decision-makers.

The recent KPMG-Forbes Annual Survey on business transformation demonstrated the continuing impact of disruption and innovation, as leaders search for more efficient ways of deploying technology to power change initiatives in their organizations. The expectation among citizens that government provide similar technology solutions as private enterprise has also opened up a new set of challenges, along with a corresponding need for more customer-centric transformation strategies. Finally, the search for fresh insights to keep up with the pace of change has prompted leaders to seek lessons from governments in other jurisdictions, with many wishing for greater insights into emerging trends and best practices.

With *@gov*, we want to start a conversation that challenges the way you think about the most pressing issues in government and public sector leadership. We will aim to provide insight and analysis that is relevant, timely, easily digestible, and can be usefully applied in a public sector setting. Above all, we want a dialogue with you so we welcome your feedback and input.

The theme of this issue is 'Transforming government in the age of technology' and topics explored by our professionals include digital identification and the challenges of implementation across key jurisdictions, the public policy imperatives surrounding the rise of autonomous vehicles, government data sharing and the balance shift from privacy toward protection, in addition to cyber security and government vulnerability to cybercrime.

I'd like to thank you for joining us on the first phase of this exciting journey. We hope that you find value in *@gov*'s content offerings as the magazine continues to grow.

If there are topics you'd like us to address or if you have comments or questions about anything you read here, please feel free to contact us at government@kpmg.com.

Nick Chism
Global Chair, Infrastructure, Government & Healthcare
Deputy Head of Global Sales & Markets

@NickChism_KPMG

What does it take to achieve digital ID for citizens?

Dean Grandy, KPMG in Australia

Today's citizens expect seamless online access to public services. For this to happen, all agencies at all levels of government should be aligned and data privacy and security assured.

We all interact with government in various ways. It could be filling out a tax return, making a claim for welfare benefit, enrolling our child at school or simply finding out what day the garbage collector calls.

We're starting to do more and more of these transactions online and on our hand-held devices. This reflects a growing recognition that citizens are 'customers' who expect the same ease and speed of service from government that they currently enjoy from leading commercial providers.

To make service digitization a reality, many governments around the world are seeking to introduce digital identities (digital ID) for every citizen.

Digital ID involves more than simply storing personal details online. It's an entire infrastructure for creating and maintaining citizens' digital identities and ensuring they can access government services efficiently and securely.

Choosing the model that works for you

When it comes to digital ID models, one size doesn't fit all. The approach must sit within national structural, legal and cultural parameters.

In my home country of Australia, for instance, the recently established Digital Transformation Office (DTO) aims to move many government services online. With its 'Tell Us Once' solution, every Australian citizen will enter key personal information into the system one time only, creating a record for all future interactions.

Estonia has by some distance the world's most highly-developed national ID card system, incorporating travel within the EU, health insurance, e-prescriptions, public transport, voting, proof of ID and taxes.

For larger countries, a more applicable example could be the UK, whose 'gov.uk' system offers secure sign-in to a range of digital government services.

An intriguing alternative is New Zealand's 'RealMe,' in which a single ID can be used with both public and participating private sector organizations. Activities as diverse as opening a bank account, applying for a student loan or enrolling to vote can all be done via the same ID.

Overcoming obstacles to implementation

Whichever approach a government chooses, the road to digital ID is paved with significant barriers:

Security and privacy

Many of us are worried about our personal details being held centrally and accessible by multiple agencies. Well-publicized leaks by both private and public sector organizations have only added to this anxiety.

Governments are keen to reassure users that their details are safe and secure. The UK has addressed this issue with its 'gov.uk' secure authentication model, in which citizens enter via a central hub and are directed to the relevant department or 'service provider.' Although the actual ID is stored on the records of each service provider, crucially, the details of each individual session are not retained, to ensure that security and privacy requirements are met.

With citizens frequently using smartphones and tablets to access services, authentication methods, such as biometrics could offer a relatively safe way into the system.

Political appetite and environment

Many countries have multiple layers of central, regional and local government. If there's a lack of legislative harmony, different tiers of government could opt out of digital ID, preventing comprehensive access. Significant variations in data quality between government agencies are widespread, making information sharing extremely difficult.

If citizen ID is to be truly government-wide, every agency will ultimately have to buy into the program and agree on appropriate legislation.

Common principles and standards for how government (and any third parties) use the ID, share data and manage security and privacy are also required. This means reaching a sensible balance between accessibility on the one hand and security/privacy on the other.

An example of this is the development by the DTO in Australia of a National Trusted Digital Identity Framework, designed to ensure consistency of approach to identity, authentication and authorization across all government services. This will also limit the requirement for multiple digital credentials.

Interoperability

Over the years, various parts of government have acquired disparate IT systems, some of which are 20 to 30 years old. In many cases, they have never interacted with each other. When a citizen wants to access a new service, they have to re-enter their personal details and different departments may not be able to access important information held by other agencies.

While it may not be feasible to expect every agency to invest in exactly the same software, it should be possible for different systems to 'talk' to each other. An 'application programming interface' (API) offers this capability by enabling free flow of information between the different applications used by different agencies.

The case for digital ID

We can all benefit from digital ID. Individuals and businesses will be able to access services easier and faster, and feel they are in control. Government can drive efficiency through better coordination and slash costs by moving to self-service, reducing the need for manual entry and re-entry of data. A more secure, consistent access method could also help save money by reducing social security and tax fraud.

The Australian Prime Minister, Malcolm Turnbull, is so serious about digital ID that he made it part of his personal portfolio. That's the kind of commitment necessary to implement this much-needed development. Governments with similar ambitions will have to be equally focused and resilient.

Dean Grandy (dgrandy@kpmg.com.au) has a long and successful track record of working as an advisor to the Australian Federal Government on technology-enabled business transformation engagements.

Five ways for governments to tighten up cyber security

David Ferbrache, KPMG in the UK

In creating a safe, digital environment for citizens and companies, government can embrace leading practices from the private sector and encourage employees to be more cyber-aware.

In many countries, citizens and businesses are using online government services to fill out tax returns and apply for housing or other welfare benefits. Each year, more and more services are going digital, from vehicle registrations to healthcare.

But what if a criminal or a malicious hacker manages to get hold of personal or company details?

In my blog post *How vulnerable are governments to cyber crime?,* I discuss how the move to digital services is opening up opportunities for organized gangs to acquire personal and corporate identities and use this information to steal from the public purse. Any interaction that involves a transfer of money will be on criminals' radar, such as tax, VAT/GST and benefits.

This is a serious and growing threat. In this blog post, I outline five recommendations for tightening up governments' digital defenses:

Treat cyber security as a critical organizational issue

Digital security isn't just something you can leave to the IT specialists. It affects everyone working in government. In the best examples from the private sector, leaders champion education and awareness of cyber security and present the risks in real-life terms so that everyone understands what's at stake and how it affects their daily jobs.

Take the oil and gas industry, where personal safety has long been paramount. Companies in this sector have tried to make cyber security an equally central part of their culture — alongside safety and not just a 'compliance' issue. Employees are encouraged to think about what kinds of assets are at risk and how they can prevent attacks and spot threats.

Governments need to adopt a similar mindset and make cyber security part of 'the way we do things around here.'

Embed more security into your supply chain

Today's governments are often heavily dependent upon a wide and complex web of service providers and contractors. With so many parties processing confidential information, the chances for leaks or theft are much higher. The best way to counter this challenge is by tightening up procurement. Contracts should embed cyber security. Ideally, suppliers should all be certified to an industry standard. Regular monitoring and independent audits can reassure government that standards are being maintained to avoid weak links in the chain. Most importantly, make sure contracts drive the right behaviors when responding to a cyber security incident, ensuring openness, transparency and a willingness to work together when the worst happens.

Encourage innovative cyber security solutions

If governments want to realize the savings and efficiencies from going digital, they need to constantly keep one step ahead of criminals. Gangs are clever and fast. As soon as one route gets blocked, they work to find another. Governments have to be even more nimble to come up with innovative and cost-effective ways to block cyber crime and frustrate the efforts of criminals to cash-out and monetize stolen information. New technologies, such as biometrics, analytics and virtualization can play a part — but so can education and awareness.

Unfortunately, many public sector digital crime prevention projects become large, expensive undertakings that don't always deliver.

It's definitely worth looking at how the private sector approaches this challenge. Financial services companies, especially banks, often create smaller, less costly 'incubator' teams with the freedom to try out offbeat, innovative ideas. They're accustomed to the digital threat and have a good record of pioneering anti-fraud measures.

Banks also adopt a philosophy known as 'fast to fail,' which halts unsuccessful projects quickly, before they consume too much money. By following this example, governments could become more agile and develop systems that spot threats early and prevent breaches.

Collaborate with the private sector

Given the success of other industries in combatting cyber crime, government should consider harnessing some of this expertise and experience. Collaboration can bring in fresh, external thinking as well as providing challenge, benchmarking and peer comparisons. We bring our clients together to provide safe spaces for discussion, swapping war stories and finding inspiration in each other's experience. The global I-4 conference programme is just one example of our work in this area.

Being prepared to share intelligence on actual and potential attacks also matters. After all, the kind of information floating around the criminal fraternity is often stolen from, and used against, a combination of public and private organizations, so it's in everybody's interests to work together.

Plan your talent needs carefully

Cyber crime is a growing phenomenon and people with the skills to combat this threat are in high demand. Today's governments can't compete with private sector salaries so it's hard to keep hold of the best talent. Workforce planning should assume that specialists may only stay for a few years and look to create a production line of new, young talent to succeed them.

In future, governments should widen their collaboration with private companies to include talent sharing. Cyber security specialists could rotate roles between the public and private sectors as part of their natural career development. It wouldn't just help government, it would also give these individuals a higher personal profile.

When it comes to physical security, we're all alert to suspicious activity. In future, government employees should all see themselves as being on the front line of identifying and responding to cyber crime.

Read David's companion interview *How vulnerable are governments to cyber crime?*

David Ferbrache
(david.ferbrache@kpmg.co.uk), was previously Head of Cyber & Space at the UK Ministry of Defence and has more than 25 years' experience in technology risk and information security.

Autonomous vehicles: the public policy imperatives

Richard Threlfall, KPMG in the UK
Scott Rawlins, KPMG in the US
Gary Silberg, KPMG in the US

It is 2025 and autonomous vehicles (AVs) are a fact of life.

Many drivers are still behind the wheel of their 'classic cars' but the switch rate to autonomous is much faster than predicted. Indeed, those still driving are feeling embarrassed by their choice, because society is increasingly intolerant of any road accident, particularly those involving injury or fatality[1].

Personal mobility has soared in the AV world, with the young, old and disabled rapidly taking advantage of their new freedom[2] and working on the move has become second nature. The country is experiencing an economic boom from the resulting rise in productivity[3], polls show social happiness has increased from the advent of what is widely known as 'stress-free AV' and there has been a small but noticeable improvement in public health, reducing strain on healthcare services.

This is not a controversial scenario to propose. Spending on technological investment in AV is now huge[4], and the potential benefits self-evident to all except the most ardent motorhead.

In any event, it is pointless debating the merits of AVs because they will happen. The only uncertainty is precisely how long it will take before AVs make up the majority of vehicles on our roads. Estimates vary but nearly all cases suggest less than 20 years[5].

What does this mean for policymakers at national, state and city level, for city transit authorities and national road authorities? They need to recognize the huge ramifications for how cities and countries will work and their ability to influence some of that destiny for a better outcome for society.

There is an imperative to act now across a broad range of public policy design and implementation issues. Act now so our countries and cities are AV-ready in time. Act now to ensure that investment decisions in our public realm and transport infrastructure anticipate the benefits that AV will bring.

Richard Threlfall (richard.threlfall@kpmg.co.uk) is KPMG's Global Head of Public Transport and also the Head of Infrastructure, Building and Construction for KPMG in the UK.

Scott Rawlins (rrawlins@kpmg.com) is a Principal in Infrastructure Advisory, Scott assists agencies with operational performance strategies and strategic asset management initiatives.

Gary Silberg (gsilberg@kpmg.com) is National Sector Lead Partner for the Automotive Industry with KPMG in the US, advising major domestic and multinational companies on investment and acquisition strategies, divestments and joint ventures.

[1] *Automobile insurance in the era of autonomous vehicles*, KPMG in the US, June 2015, suggests accident frequency could drop by 80 percent.

[2] *The Clockspeed Dilemma*, KPMG International, January 2016.

[3] *TSLA's New Path to Disruption, Morgan Stanley, February 2014, and Autonomous Cars: Self-Driving the New Auto Industry Paradigm, Morgan Stanley, November 2013* Reference US, Canada and UK economic benefit forecasts.

[4] *Autonomous Driving: Question is When, Not IF, IHS Automotive*, updated January, 2015.

[5] *IHS Autonomous sales forecast*, IHS Automotive, December 2014.

There are five areas in particular where AVs have significant implications for public policy and service:

1. Transport infrastructure investment decisions

Accountability for taxpayers' money demands that our public investment decisions are founded on robust cost-benefit analysis. The cost is incurred now but the benefit is typically appraised over a 30 to 50-year period. It is a certainty that AVs will have changed our society within these timeframes. So value for money analysis on transport schemes today should already be based on an AV world. This will affect decisions on which schemes are the highest priorities, and for those schemes which progress, it will change their design and, hence, their cost. As an example, an AV road is unlikely to need the crash barriers or hard shoulders of today and the lanes could be much closer together, saving significant land use and cost.

2. Licensing and road traffic regulations

In an AV world, there are no drivers. So, ultimately, no need for driver licensing. However, in many countries, driving licenses also operate as citizen ID. So the implications of withdrawal need to be thought through. Timing is also a consideration. In the initial years of AV adoption, it is likely most countries will continue to require that a licensed driver can take back control of the vehicle. But, eventually, trust in the technology should mature so that is no longer necessary. Then, there is the licensing of vehicles. Will that still be necessary? From a safety point of view, would it not suffice to put the onus on manufacturers to produce safe products, as is the case for nearly every other consumer good, rather than have a regular testing regime? But vehicle registration may continue to be needed as the basis of revenue raising from AV use. Finally, traffic regulations will need to be adapted and, in a pure AV world, replaced by connectivity standards, operating like internet protocols.

3. Revenue

AVs will still need roads on which to travel, and expensive investment in digital technology to provide the bandwidth for vehicle-to-vehicle and vehicle-to-infrastructure communications. Cities are likely to want to establish control centers so they can intervene to minimize congestion. The AV revolution creates an opportunity for governments to rethink and improve the funding models for road infrastructure. There is a choice as to whether that infrastructure should be built and maintained by the public or private sector. Perhaps all the communication systems, for example, should be left to the market to provide. But where the public sector is paying, new forms of vehicle or usage taxes will be needed to replace the loss of taxes from fossil fuels[6].

4. Spatial planning

AVs offer not just a revolution in transportation, but also in how we live. Mobility on demand without the need to own a vehicle means accessibility for all, a huge increase in vehicle miles[7] travelled but potentially much higher levels of vehicle utilization[8]. We may need fewer vehicles and if we don't own that vehicle we don't need to park it. In dense urban environments, garages and hard standings may become a thing of the past. AVs will also be able to pass much closer, so many roads could be narrower. Residential streets could serve both AVs and pedestrians in the same space without the need for curbs. We will face new choices about how we shape our urban environments, and how we use the huge amount of space that could be released.

5. Security

In a world of AVs, we put our lives in the hands of the systems which control them. We will expect assurance that those systems are failsafe and safe from malicious attack. Governments will need to establish regulations for the systems, as well as regular testing regimes. Accident rates will reduce dramatically, and, if combined with reduced levels of personal vehicle ownership, will transform the car insurance industry[9]. Personal data security will also be a concern, as AV payment systems are likely to rely on detailed knowledge of where we travel.

Public authorities need to start planning now to navigate through these myriad issues and ensure that our AV-dominated world is one designed to maximize social and economic benefit.

In upcoming *@gov* features, we will explore the key issues in more detail, helping authorities to start to envision a blueprint for the design and implementation of an AV-powered community of the future.

The potential benefits of AV are huge. Let's start planning together now to make them a reality.

---

[6] *US Motor Tax Fuel Revenue, 1977-2013*, Tax Policy Center; *Tax and NIC receipts: statistics table, HMRC Tax Receipts and National Insurance Contributions in the UK*, HM Revenue & Customs, October 2013.

[7] *The Clockspeed Dilemma, KPMG International, January 2016.*

[8] *Autonomous Vehicle Implementation Predictions, Implications for Transport Planning*, Victoria Transport Policy Institute, August 2013.

[9] *Automobile insurance in the era of autonomous vehicles*, KPMG in the US, June 2015, estimates that the personal car insurance market could fall to 40 per cent of its current size.

KPMG

@gov

Inspiring innovative government

Get inspired
with @gov email updates

Email government@kpmg.com to be added to our mailing list.

kpmg.com/atgov

Sharing government data for a better world

Eric Applewhite, KPMG in the UK

We all respect the need for data protection. But if we want to offer better services for citizens, we need to strike a balance between data privacy and our public duty to enhance and even save lives.

Sometimes you hear a phrase that says it all. The Farr Institute's #datasaveslives campaign does that for me. In highlighting the positive impact of data research on public health, its simple message reminds me why our continued dialogue about data sharing is so important. It's about lives and well being and using information creatively but responsibly to help others.

I worry we have the balance of that conversation wrong in the public sector — and it isn't entirely our fault. We're influenced by values that are so important to our culture, and by a legal system that, taken to an extreme, can actually create a disincentive to even start conversations about improving lives with data, because it's too risky or too difficult.

Why do discussions about data sharing for the public good feel so much like trench warfare? Why are they so hard to sustain? How come we trust big companies to take care of our data, yet push back on government data sharing programs? That has to be wrong — doesn't it?

When I lived in New York, I heard about a mother and her two young daughters evicted from their apartment. They faced an uncertain future in sheltered accommodation. Fortunately, their case worker was able to quickly access the family's welfare records, which soon got them settled in new housing. Surely, that's what good data sharing is all about. I don't think many people would argue with that.

This story demonstrates just one of the many ways in which data sharing can make people's lives better — and make government more efficient and effective. There's so much to gain in the form of early intervention and prevention, better targeting of services toward those most in need, and a move toward efficient, self-service for citizens — all underpinned by simplified business policies.

Sadly, the reverse is also true. When government agencies can't exchange information, citizens sometimes suffer and costs can rise. So you can get

caseworkers failing to spot people who need support or who are at-risk. And countless hours can be wasted on unnecessary administration; hours that could be better spent providing service and care to people.

Shift the balance from privacy towards protection

What I've noticed is that some attempts to share citizens' information to improve well-being can be held back by a hesitant and sometimes too conservative information sharing culture. The laws and processes so important to us have the unintended consequences of making it harder for governments to share when they are allowed to and expected to by those they serve. After all, why take the chance of sharing when one accidental or intentional breach can undo the impact of a thousand data sharing success stories — especially if it's in the public eye.

This fear stems from a system skewed towards the consequences of poor sharing and away from the benefits of positive sharing. Both are important, but it seems to me we've got things the wrong way around. We should *begin* with a duty to share and balance that with a duty to protect privacy. A proportional and balanced conversation about both aspects of protection privacy and safety should be the norm, not the exception. That balance cannot happen without strong leadership to sustain an information sharing culture change.

I was recently at a workshop with health leaders discussing barriers and opportunities in the UK health system. A participant summed this up better than I ever could when she said: "I'd rather be held to task for sharing data when I shouldn't have, than have to answer for why I didn't share data when I should have. There's simply too much at stake when it comes to our patients."

All around us we're starting to see strong demonstrations of this kind of leadership, along with shifting attitudes towards information sharing. I'm inspired by organizations like the Farr Institute. They remind us that improving lives is what matters and that we shouldn't be apologetic about using data to this end.

Globally, you need look no further than the UK's Office of the National Data Guardian and New York City's Executive Order 114 (PDF 16.3 KB) for Health and Human Services. Both empower the public sector, and both place sharing data for the public good in a proportional rational balance with protecting privacy. By supporting proportionality in data sharing decisions, they remind us to seek opportunities to share — as long as we can find a valid information sharing path in law and statute seeking consent when needed.

The overriding message is: 'set out and try' rather than 'make sure you don't fail.' This is a great example of 'whole system leadership,' which can help create a collaborative, problem-solving, data sharing culture; one that recognizes the many advantages to government and its citizens and is motivated to overcome barriers if it helps others.

It's this kind of mindset that's driving a major UK data sharing and collaboration program, where our KPMG in the UK member firm is worked with the city of Manchester to reimagine how it can better share information as a whole system for the public good and build an incremental capability that increasingly puts its residents at the center of decisions about what to share and when to share.

'Greater Manchester Connect' aims to create an organization-wide framework for data sharing, with common governance and standards for all its agencies. Its job is to build trust and an information brokering capability across a diverse set of programs and geographies, supported by strong, accountable leadership to maintain momentum.

Some of the thinking behind this initiative was influenced by another highly successful data sharing program in New York City that our KPMG firm in the US assisted with. '*Health & Human Services Connect'* (HHS-Connect) didn't just have inspirational leaders, it also had an information governance team including lawyers and analysts who together mapped out an information sharing path.

To me, they were data sharing pioneers who bought into the vision and, in the words of one team member, were prepared to 'test it and kick it hard' in order to find data sharing solutions. Because that's what their citizens expected. They were pragmatic as well, targeting an ambitious success rate for their data sharing efforts. Equally, they acknowledged that some kinds of data are too private to share and that sometimes validating that data shouldn't be shared was as valuable as finding a way to share it.

Eric Applewhite (eric.applewhite@kpmg.co.uk) has over 20 years' experience in technology and information sharing engagements across North America and Europe, focusing in the Health and Social Care sectors.

Start with defining benefits

There's no escaping the fact that data sharing can be controversial so it's vital to quantify the benefits to strengthen your argument. A benefit estimate and realization model is a good way to consider the entire cost of the program. This can then be compared to the value of future efficiencies and savings, like less time spent on administration, more efficient case management and lower care costs due to early intervention. Program managers have to track costs and savings to assess progress and justify the investment.

But it's not just about numbers. It's equally important to measure the outcomes in terms of improved quality of life for citizens. In New York, a series of outcomes were tracked, like improved mental, physical, and nutritional health, lower homelessness, and better child well-being and family stability. These kinds of improvements should ultimately improve outcomes for residents and reduce costs of care.

This kind of investment in the front of the process answers the question: 'why should data be shared?' and should pay huge dividends. When inevitable conflicts about information sharing arise, measurable benefits help refocus everyone's attention to what really matters: the human and economic value of sharing.

The alternative? To wait for an adverse event — like the death of a child, a natural disaster or a terrorist attack — to highlight data sharing inadequacies. But who wants that? Surely, it's better to think of ways to prevent bad things happening in the first place.

Build a federated capability

Then, there's the question of who controls the data. Programs may wish to store all the information in one place to produce amazing insights. But each agency may feel a strong sense of ownership about the data they hold and be reluctant to let it sit outside the department for both legal and cultural reasons.

In our experience, it's better to avoid a protracted fight over ownership. A smarter and more practical alternative is to create a sophisticated 'data federation' capability, where information can be made accessible to other agencies but remains the possession of one agency. Access to that data can be safely controlled by program and role-based security at the technology level, giving confidence that only allowable sharing is occurring. You can complement this approach with a centralized data analysis facility that can draw on data from participating agencies and systems.

From blockers to backers

Because data sharing is typically seen as 'administrative and risky,' those overseeing it are often compliance-oriented and risk-averse. Media stories about leaked personal details only make them more guarded. But these people are also deeply passionate about protecting citizens and getting things right.

For me, one important step is turning our information governance professionals into information sharing 'coaches.' A fresh approach is needed, where they can put their arms around us and help us navigate the risks and opportunities in each data sharing path. This means trusting and supporting them as important members of the leadership team. By giving them the chance to look at opportunities early, these professionals can start to see sharing as a problem to be solved rather than a path too risky to be crossed. Empowered information sharing coaches can become the cavalry for a new kind of information sharing culture. They will save the day when information you should share and are allowed to share is threatened by poor process or inertia.

Putting citizens at the center

We can't forget the role that citizens play in data sharing. After all — it's about them and we're mostly talking about their data. But all too often, public sector agencies go about seeking consent in the wrong ways. In many instances, requests to share are delivered from a position of negativity or neutrality and that doesn't work. Instead of asking: "Will you donate your kidney when you die?" why not say: "Do you want to give someone the chance of a new life?" The private sector has mastered the knack of using value to gain consent and government should also embrace similar cognitive and 'nudge' techniques to accentuate the positive and explain the value from sharing. We also need to make the actual opt-in process as quick and easy as possible while explaining why citizens should want in not out. Luckily, nudge and behavioral techniques are increasingly becoming a core part of a proportional and human conversation with residents about what is in it for them.

Transparency is also the key to winning public trust and consent. Governments need to state clearly how they plan to use data. And to establish trust, personal details should be accessible to citizens, so they can see what data is held, and correct or update their records. It goes without saying that the system should be accessible to all types of mobile devices, using the most sophisticated identity verification and cyber security investments possible. By 2020, more than two-thirds of the world's population will have a smartphone[1], which is rapidly becoming the main vehicle for all online activity[2]. We should be testing consent models and approaches using mobile devices today, as people are already getting comfortable with this medium. Mobile communications are also making it easier to explain the value of sharing.

My glimpse of the future envisages government increasingly helping citizens to understand and control their digital identities. We'll see more and more personal data stores used by citizens to manage their own data and consent online. Mydex (a personal data store controlled by the individual) and Hub of All Things (the HAT — a platform enabling individuals to trade and exchange their personal data) are good

[1] The number of smartphone users in the world is expected to reach a giant 6.1 billion by 2020, Digital Trends, 3 June 2015.

[2] In Less Than Two Years, a Smartphone Could Be Your Only Computer, Wired, 2 October 2015.

examples of what's emerging in that space today. And increasingly, we're all seeing government's role as an information broker and steward for the public expand, especially as it relates to exposing 'open' and public data for value. Places like Leeds and London are leading the way in this space in the UK along with Data.Gov in the US. Copenhagen is taking a step further to become one of the first public sector entities I'm aware of to try and monetize its public and private data in a citywide information marketplace. This may be a bridge too far for you or it could be a glimpse of the future where controlling and getting value from our 'digital' selves is something worth investing in and paying for. It is clear to me that governments need to be thinking about their roles and responsibilities as a societal information broker in new ways. Things are changing and they need to be ready to help residents and citizens meet, manage, keep safe, and 'optimize' their digital well-being. Not everyone will land in the same place about how far the public sector needs to go but the time for beginning to develop your position is now. What's at stake is a completely new relationship between citizens, governments, and data.

Because governments are at the heart of information and the public trust, I believe governments are uniquely positioned to accelerate this process. In fact, they have a duty to do so. Public sector chief information officers, chief executives and other leaders should be looking at this trend now and getting ahead of the wave. If we can entrust our most intimate details to big corporations, surely we can view the public sector as a truer custodian? After all, governments and their agencies are not generally seeking to gain commercially. Their prime interest is in improving citizen outcomes and making themselves more efficient (which also benefits the public). If they can help citizens take control of their own data, it should be easier to get them to consent to data sharing, as they'll see the value it brings.

When they share data, governments gain a more holistic, 360-degree view of citizens and their families. They can understand peoples' needs more clearly in the place that they live and focus on prevention and earlier intervention to improve service and prevent harm. All of which should mean more efficient use of resources, an improved experience for citizens and better outcomes for individuals and society. Privacy and confidentiality will always be high on the agenda. But, as the examples in New York and Manchester demonstrate, there is an opportunity to create a proportional and impactful information sharing culture, by being more positive about data sharing and emphasizing how it can help create a better world.

7 strategies for more effective government data sharing

1. Foster a collaborative, problem-solving culture for data sharing, focused on delivering human and economic value.
2. Assemble an empowered information governance (coaching) team with a strong, accountable leader.
3. Establish trust and a common language for sharing via common data standards and data sharing agreements.
4. Be positive on data sharing, by pushing hard for creative solutions that engage citizens and offer real benefits. And accept that some sharing initiatives won't succeed.
5. Make your system transparent and 'citizen friendly.' Prepare to be positively surprised by what you hear.
6. Invest in benefits realization, to measure economic and more qualitative outcomes. This creates the foundation for sustained conversations with your residents and employees about sharing.
7. Embrace the concept of 'data federation' to preserve data sovereignty and encourage sharing within agencies.

GOV.UK sets a high social media standard

A conversation with Georgina Goode of the UK's acclaimed Government Digital Service.

Described by former British Prime Minister David Cameron in 2015 as "One of the greatest unsung triumphs of the last parliament," the Government Digital Service (GDS) has since garnered much praise for driving the digital transformation of the UK government.

Established in 2011, GDS has helped the Cabinet Office apply technology and innovation to reinvent the way the state delivers public services, in part through GOV.UK, a central website for all government departments.

Georgina Goode joined GDS in 2014, as Head of Social Media, to devise content and community building strategies to engage the public in UK government's new digital public services. In light of her team's success in growing traffic to GOV.UK, we spoke with Georgina about her work and to learn her views on ways governments can best leverage social media.

How would you describe your group's approach to social media for the UK government?

GG: We see social media as very much an extension of great service delivery to our GOV.UK platform, in terms of how we engage users, design new content and provide data and insight.

Our role is to signpost users to the right information at the right time, to provide support, as you would expect from any online service and to provide data and insight to wider teams across GDS, for example GOV.UK operations teams, user research and GOV.UK content teams. This is so, what we learn from our users on social can be fed back into wider programs of work, designed to make the delivery of government services even better. We very much embody GDS's core principle for digital transformation — helping support the delivery of services that are 'Simpler, Clearer, Faster'.

Tell us about the primary social media channels you use at GDS:

GG: The bulk of our social activity takes place on Twitter, of which we have two accounts, each with distinct audiences, depending on whether we are communicating public service announcements, new regulations, program information, etc. Among them, we operate **@GOV.UK**, which is one of the largest government Twitter feeds in the UK.

We also leverage channels such as YouTube, Flickr, and LinkedIn, particularly as part of our corporate work on behalf of GDS to communicate with audiences such as wider civil service, media and the digital and tech industries. We continually push ourselves to improve and test new tactics, especially to invite user interaction and feedback that can bring value to other teams across GDS. We've seen great results, such as growing one of the largest Periscope communities in government for our expert Q&As and achieving impressive LinkedIn user engagement scores that far exceed the industry average. It shows that when you've got great content on the right channel, it can be extremely effective for audience engagement.

So you believe that social media has a role to play in supporting government service delivery and improving operations?

GG: Absolutely. Social media is where users come to ask questions and, of course, vent. There definitely is a user expectation that service providers are present on these channels and governments around the world can't ignore this.

That said, it's important to understand that social media is not going to fix services that are broken or poorly designed. In fact, it will only make things worse. That's why we are so focused on providing data and insights from social media, in supporting other research sources, to help understand user needs and constantly improve service delivery. It's all well and good to shout from the rooftops about your digital services but, ultimately, it's the services that need to speak for themselves, by working well and fulfilling user needs.

Can you give an example of a social media campaign that shifted user behavior?

GG: A good example of this is how we are bringing government transactions into the social media newsfeed. For instance, 2015's General Election — we wanted to drive traffic and registrations to the new Individual Electoral Registration service, which was replacing an outdated household registration process. The service itself is fantastic and meant users could register their details in under 3 minutes.

We tested a series of Twitter Cards with strong calls to action, imagery and trackable links. From one card alone, we were seeing conversion rates of 30 percent — that's users clicking on the card and completing the registration process right there and then, in that moment. And that's organic traffic with no spend on advertising.

That figure is pretty staggering and shows the possibilities available to governments in using social media to help get users to the services they need. Making a user journey not only simpler but more convenient.

How would you rate most governments' social media efforts and what must they do to catch up to the private sector?

GG: It depends on where a government currently sits on its digital transformation journey, since social media is one small part of that. I would say that most governments appear to recognize the importance of using social media far more strategically than in the past.

In terms of 'catching up' with the private sector, we have some of the best digital talent working within GDS as well as across government and GOV.UK as a platform and our social media output is better than a lot of what you'll find in the private sector.

That said, whether public or private sector, the quality of an organization's social media ultimately boils down to its overall ambition and willingness to make social an intrinsic part of the business. If that ambition isn't there, it's not going to work, whatever sector you operate in.

But does government face unique cultural or organizational barriers to using social media?

GG: It's really about whether they are ready to embed digital across the organization. That's a big challenge for any large organization, including a government ministry/department with many hundreds of employees. It must fundamentally change the way it works, including rethinking internal structures, up-skilling its people, or bringing in new digital talent to help. It's not easy, but the UK government is doing it, and there is amazing work underway by governments around the world.

But doesn't social media pose additional risks for governments?

GG: The truth is there's greater risk in not doing this stuff than there is doing it. However, governments must be well-prepared to deal with the challenges and scenarios that could potentially come up. That means having comprehensive risk management systems, clear escalation procedures and strict behavior guidelines for your social media communities. It's about planning and having the right procedures in place.

What about the challenge of keeping up with the very dynamic social media environment?

GG: The social media landscape is in constant flux. That's a given but, importantly, user behaviors are changing and content needs to be driven by this (user needs not government needs). It's no longer about pushing out content for content's sake or jumping on the next shining new platform bandwagon.

Can you suggest some best practices for governments on social media?

GG: I'd sum up my advice in five broad areas:

1. Have a clear strategy with defined objectives and benchmarks to measure your efforts for continuous improvement and to compare yourself against others.
2. Perform extensive user research and planning and take advantage of digital and social monitoring tools to understand your users, their needs and expectations, as well as the channels and tactics available to you.
3. Start small and build from there, aligned with a long-term vision. Focus on a particular service before rolling out a huge social media plan for an entire department.
4. Avoid operating in silos to ensure you have all necessary stakeholder input and support. In government, include the policy, campaign and operations people, and don't limit group representation to people with 'digital' in their titles.
5. Finally, build a brilliant content team, from planning specialists to writers and designers, because social 'lives and dies' on the quality of its content. And ensure your team has clear digital design guidelines and principles to follow in place.

What's your next major focus at GDS?

GG: I'm very focused on ensuring we stick with our strategy and maintain standards. I firmly believe that, as government, we have a responsibility to our users to only deliver the very best, so there is little room for error.

We also continue to test and push video and live-streaming tactics, plus we are looking into strategies that focus on multi-platform delivery. This is a very interesting space for us — looking at how else and where else users can now access government services and how we can create a seamless experience across all those channels. The opportunities are really endless when you see the number of services government provides and it's fertile ground for us. A lot is happening so watch this space!

Useful links:

UK government's Social Media Playbook

GDS Design Principles

@GOVUK

@gdsteam

@GeorgieC

Innovations in human services delivery

Liz Forsyth, KPMG in Australia

Smartphones, mobile apps, social media, cloud data solutions. Technology is profoundly changing the way we live, communicate and interact. It is also transforming the provision of human and social services, offering new ways for governments to deliver services and connect with citizens.

The pace of change is staggering, a trend that is forecast to continue — and which presents enormous challenges and opportunities for governments.

Tight budgets are often a motivating factor for technological change: the mantra of doing more with less is pervasive. But government leaders also want to do more to help their constituents: not only those with the most pressing needs — such as the homeless, at-risk children, senior citizens, people with developmental challenges — but all citizens who want their interactions with government to be convenient and quick.

@gov will be exploring these themes in a series of articles published over the coming months.

The challenges of digitizing human services

Governments are bulky, complex, and vast. Their huge scale and multifaceted mandate has traditionally been managed by developing a layered organization from top to bottom — from national to local — and populating each layer with innumerable departments, each with a different focus. That has created significant structural and operational challenges.[1]

With great size comes an institutional aversion to risk and the monopoly position of governments can mean they lack incentives to deliver the best, most innovative services in order to retain their customers. The citizen, after all, cannot go elsewhere for the same service.

With the imperative to compartmentalize comes a silo mentality, as departments develop unique processes and customized IT solutions. And although budgetary pressures sometimes force innovation, they can also encourage a tendency to stick with outmoded technology and procedures.

Now, governments risk being left behind if they continue to provide services as they did 50 or more years ago. Fortunately, while the challenges of embracing new technologies are temporary, the opportunities are already with us and the benefits are long term.

The benefits of digital innovation

Technology is enabling the exchange of information on a previously unimaginable scale, allowing related government agencies and external service providers to share data and coordinate their efforts. It is also providing governments with far more data than ever before about what citizens need, who uses government services, how they do so and with what effect.

As delivery modes advance and the varying impact of services is better understood, new technology is making services much more efficient and effective. Among other topics we'll explore in our series are two highly promising technological developments.

[1] These observations are drawn in part from Forbes Insight, *Digitizing Human Services: Field notes and forecasts from the front lines of government's technological transformation* (2015)

Mobile apps

We will look at the power of mobile apps to improve service delivery in myriad ways: supporting vulnerable citizens, delivering counselling and improving child care practice, to name just a few. The technology benefits citizens very directly, too. Mobile apps allow them to register for services, claim benefits, and update their information — all without having to visit an office or wait on the phone.

Research has already discovered that citizens in need are more likely to use mobile technologies than they are to turn to the web. Harnessing that trend can improve the lives of citizens across a spectrum of need.

Predictive analytics

We'll also explore the use of predictive analytics to better protect children, prevent homelessness and anticipate service demand.

Most governments already have information they could use to identify people in need of assistance. Geographic and predictive metadata can pinpoint citizen risk factors, and highly sophisticated data analysis can inform policy development and improve outcomes by helping providers to target and deliver services more effectively, often at a lower cost.

Strategic trends in service delivery

The expectations of citizens are clear. As they experience growing convenience in their commercial interactions — finding information and purchasing services with increasing speed and ease — they want government to have similarly contemporary communication and service delivery systems.

To meet those expectations, governments must step away from the old, compartmentalized modes and take a strategic approach to reshaping the delivery of human services:[2]

— **Integrating services and service delivery across departments and agencies:** In order to break down silos, governments have to secure commitment at senior levels, define the goals and develop appropriate processes and ways to evaluate progress.

— **Partnering with private-sector and not-for-profit organizations:** Today, innovation is coming from outside government: from academic institutions, not-for-profits and private businesses. Collaborating with these sectors will provide needed expertise and uncover best practices.

— **Creating a user-friendly portal to a wide array of related services:** Broadening citizen access is a key aspect of enhancing service delivery through unified, easy-to-use client pathways that keep the user experience in focus.

— **Tailoring solutions to specific community needs:** To avoid program overlaps, inefficient investment and ill-fitting outcomes, place-based planning must drive the way governments deliver services.

— **Developing metrics that focus on meaningful outcomes for the consumer rather than the agency:** Performance indicators need to measure the impact of services on human experience, not simply the program outputs.

These trends are essentially strands of an ecosystem approach to human and social services. By using technology to share information, connect users and services and work collaboratively across service areas, governments will optimize their resources and transform the experience of citizens.

Understanding the citizen's perspective

Information is powerful and technology delivers information to both the service provider and the service consumer. Successful innovation in healthcare, crisis services, senior services, financial aid or any other area of human and social services involves first rethinking the business-as-usual approach and then incorporating technology to provide solutions.

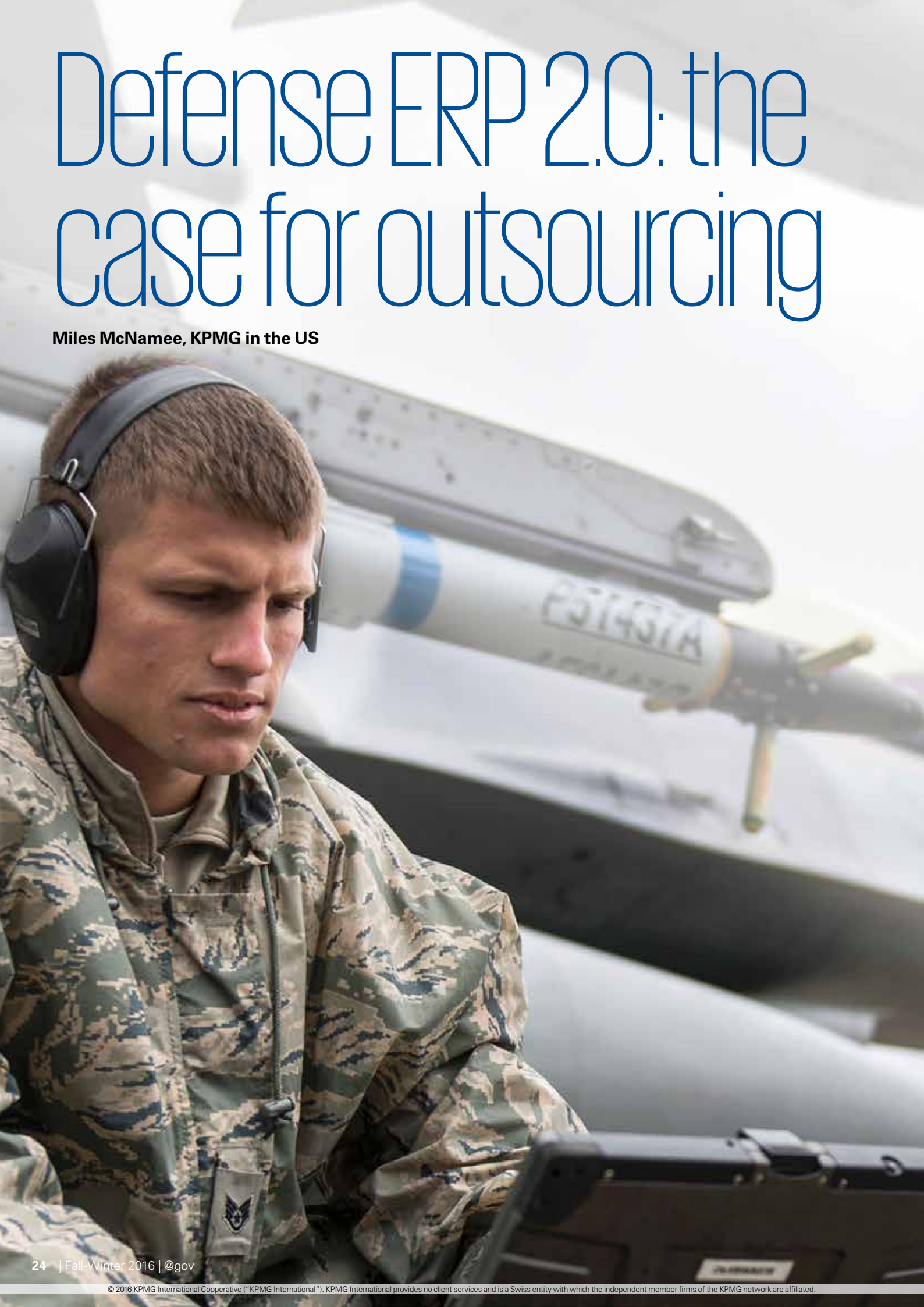
Most of all, technology is allowing government to make a transformational shift from delivering programs one agency at a time to focusing on their role from the citizen's perspective.

Liz Forsyth
(lforsyth@kpmg.com.au) is KPMG's Global Lead for Human and Social Services. Within Australia, Liz leads KPMG's National Health, Aging and Human Services practice, a key advisor to government as well as the private and not-for-profit sectors.

[2] These insights are based in part on findings outlined in KPMG International, *The Integration Imperative: Reshaping the delivery of human and social services* (October 2013), and on Forbes Insight, *Digitizing Human Services*.

Defense ERP 2.0: the case for outsourcing

Miles McNamee, KPMG in the US



The persistent march of technology leaves defense organizations scrambling to keep up with the latest innovations, and increasingly dependent upon enterprise resource planning (ERP) systems to support every aspect of their operations, from back office to the combat theater.

After long, costly, and often complex ERP implementation programs — some have been known to take as much as 5 years and billions of dollars — defense forces often find themselves with systems that fail to meet user requirements, and, worse still, have already become obsolete.

There is a better, more effective and efficient way. Rather than try to reinvent the wheel by building their own infrastructures and developing dedicated software from scratch, governments could look to the private sector to take the strain — and help relieve the pressure on federal budgets.

The logic is compelling. Companies from sectors such as manufacturing, retail, healthcare, logistics and facilities management have developed world-class processes, data centers and supply chains, all powered by cutting edge ERP. So, why try to build your own system when you can outsource from the very best?

In a public statement in 2013, the US Department of Defense (DoD) anticipates "significant use of public-private partnerships (PPPs) with "non-federal entities" across a wide range of activities that vary in scope and scale."

Today the DoD already outsources training, buildings and facilities, logistics, weapons systems, fleet maintenance for tanks and other vehicles, transportation and fuel, utilities and water. Defense organizations in the UK, Australia, the Netherlands, Mexico and France have all embraced outsourcing.

Supporting the mobile battlefield

Most of the communications on a modern battlefield involve replenishment of materials and fuel, as well as critical 'command and control' tactical decisions, all of which rely on robust ERP.

An ERP is, in essence, a huge data center, and some governments have entrusted private providers to build and operate such facilities, albeit outside the defense sector. Canada's Ministry of Government Services has a data center located in the province of Ontario, while in Brazil, an external contractor built and operates IT and telecommunications equipment for the country's private and state-owned financial institutions.

Understandably, governments are reluctant to place such 'crown jewels' in public space, and most IT outsourcing is 'inside the fence' in secure sites within a country's home borders, typically staffed by nationals only.

Given the concerns over security, will the DoD or other agencies be bold enough to extend their outsourcing to encompass that most prized asset: information?

The UK has, arguably, gone further than most, with its Government Communications Headquarters (GCHQ), which offers managed infrastructure services via a 30-year PPP, providing critical support to the government's security, defense, foreign and economic policies.

Growing use of cloud technology inevitably means accessing commercial cloud services. In February 2016 the US Defense Information Systems Agency signed up for IBM cloud services for controlled unclassified information.

The DoD has acknowledged the need to be more efficient and more centralized in its ERP infrastructure, to avoid duplication and achieve common, consistent standards. It has created a center of excellence to accelerate this shift.

These developments, though positive, still rely largely on in-house resources to manage IT — which goes against the trend in the private sector, where outsourcing has proved enormously successful in reducing costs and complexity, and raising efficiency, in the process avoiding painful implementation.

Security may be an obstacle — and one that would-be ERP providers are working hard to overcome — but, otherwise, ERP for defense is really not unique. Regardless of the organization, or the sector, many of the functions being driven by systems, such as HR, Finance, logistics and supply chain, share similar characteristics and have common user needs.

Many US military communications rely on commercially owned satellites. If the DoD can take this lead and push for outsourced ERP, then large-scale program failures could become a thing of the past, ushering in a new era of efficient, cost-effective, cutting edge operations — on and off the battlefield.

Miles McNamee
(mrmcnamee@kpmg.com)
Global Defense Lead Partner, has over 37 years' experience in managing and supervising complex projects and teams and over 29 years of highly specialized systems engineering, software development, and program management experience.

Further reading

Find more insight from @gov online at kpmg.com/atgov.

Information infrastructure security: stepping up the fight against the invisible cyber enemy.

A new EU report urges greater public-private collaboration and information sharing to protect critical information of national importance.

Paul Weissmann and Pascal Pillokeit, KPMG in Germany

How vulnerable are governments to cyber crime?

As government services go digital, criminals are spotting new opportunities for fraudulent claims and theft.

David Ferbrache, KPMG in the UK

Providing a digital welcome for migrants

With the influx of migrants into Europe, this article discusses the need to provide a more streamlined, digital approach to governmental processes.

Hartfrid Wolff, KPMG in Germany

Are governments realizing the full potential of social media?

Social media isn't just a convenient way to pass on news to citizens — it opens up a conversation that informs policy — and alerts governments to emerging risks. But how do you cut through all the 'noise' to find out what people are really thinking?

Greg Daniel and James Griffin, KPMG in Australia

Publications

To access the publications listed here, visit kpmg.com/government or email us at government@kpmg.com.

Insight: the global infrastructure magazine issue no. 8 infrastructure morality

In this edition of Insight, we focus on tackling some of the hard issues around the topic of 'Infrastructure Morality' — flash-points such as migration, economic inclusion, corruption, social equality and affordability — by asking the difficult questions of infrastructure leaders and executives at the forefront of the morality debate.

kpmg.com/insightmagazine

Future State 2030: the global megatrends shaping government

Identifies the nine megatrends impacting governments as they relate to changes in individuals, the global economy and physical environment.

kpmg.com/futurestate

Operation ready defense ERP: the backbone of today's defense capabilities

A series of thought-provoking insights on the use of enterprise resource planning systems (ERPs) in modern defense forces along with profiles of the US, UK, Australia, New Zealand and Canada.

kpmg.com/defenseERP

2015 Change Readiness Index

A ranking of 127 countries, both developed and developing, based on their ability to manage change and cultivate opportunity.

kpmg.com/changereadiness

@gov Editorial Board

Nick Chism
Global Chair, Infrastructure, Government & Healthcare
Deputy Head of Global Sales & Markets
KPMG International
T: +44 20 73118603
E: nick.chism@kpmg.co.uk

Kru Desai
Head of Government & Infrastructure
KPMG in the UK
T: +44 20 73115705
E: kru.desai@kpmg.co.uk

Liz Forsyth
Global Lead for Human Services
KPMG in Australia
T: +61293358233
E: lforsyth@kpmg.com.au

John Herhalt
National Industry Leader, Government & Public Sector
KPMG in Canada
T: +1 416 777 8500
E: jherhalt@kpmg.ca

Michael Hiller
National Partner in Charge, Infrastructure, Government & Healthcare
KPMG in Australia
T: +61 7 3233 3299
E: mhiller1@kpmg.com.au

Miles McNamee
Global Defense Lead Partner Principal, Advisory
KPMG in the US
T: +1 703 286 8330
E: mrmcnamee@kpmg.com

Mathias Oberndörfer
Leader, Government & Infrastructure
KPMG in Germany
T: +49 911 8009299-32
E: moberndoerfer@kpmg.com

Richard Threlfall
Global Head of Public Transport, Partner and Head of Infrastructure, Building & Construction
KPMG in the UK
T: +441132313437
E: richard.threlfall@kpmg.co.uk

Nancy Valley
National Government & Public Sector Leader
KPMG in the US
T: +1 518 427 4610
E: navalley@kpmg.com

KPMG's Global Government & Public Sector Practice

As trusted advisors to government organizations around the world, KPMG member firms understand the unique challenges facing today's public sector. Our dedicated, passionate and highly experienced professionals leverage our global insight to tailor smart, creative and forward-thinking solutions for local, regional, national and international public sector organizations.

www.kpmg.com/government

kpmg.com/socialmedia

kpmg.com/app

Download on the App Store

Designed by Evalueserve.
Publication name: @gov Inspiring innovative government
Publication number: 133827-G
Publication date: September 2016