Institute for Citizen-Centred Service
Pursuing excellence in public-sector delivery

Joint Councils Executive Report on Trends this Month

Government innovation, the role of the Chief Information Officer, and Artificial Intelligence in government were key trends this month.

Key insights - Government Innovation

UK - The UK government has released its highly anticipated Innovation Strategy, which sets out the national approach to digitization of the public sector. The Government Technology Innovation Strategy, launched on June 10th, outlines proposals under the themes of People, Processes, and Data and Technology. It also details ways in which government can improve coordination and cohesion around innovation based on consultations across the public and private sector and academia.

A few key highlights:

- The drive for secondments stands out as the most eye-catching initiative in the 'people' section of the strategy. Government is asked to "explore seconding senior civil service leaders to industry to allow them to witness the benefits of a culture of experimentation and empowering them to adopt these practices when they return to government".
- The 'process' segment of the strategy focuses on progress in the recent government creation of £650m Spark marketplace – a dynamic purchasing system covering 64 types of technology across various areas to improve take-up of technology.
- The data and technology section highlights the plan to "develop a detailed cross-government view of the scale of the challenge of legacy technology, put in place plans to tackle it, and make sure there is continuous improvement in our technology estate".

HONG KONG - A Smart Government Innovation Lab has been launched in Hong Kong, with the aim of supporting small and medium-sized tech enterprises and start-ups to develop products that can help improve public services. The Lab will also function to raise awareness across Hong Kong's administration about technologies that might be useful to public servants. Read more here.

Key insights – Chief Information Officers

US - GovTech gathered data for 206 state CIO terms going back to 1994 to find out more about the people leading technology in state government. A few key highlights:

- Fifty-nine percent of state CIOs' held a previous position in the public sector.
- After serving as state CIO, 52 percent of this group moved to the private sector.

- CIOs stayed in office for three years and six months, on average.

US - A recent article on the necessary skills of a government CIO argued that "the changing role of CIOs reflects what has happened on a broader scale in government IT. The era of virtualization, data center construction and overall operational efficiency is waning. The mass consumerization of technology has shifted IT's role from its primary back-office function, serving government workers, to one in which it is expected to enable a broad range of new services that can be downloaded onto smartphones and provide citizens with personalized experiences."

US - CIO Jim Weaver explains the importance of good governance, repeatable business processes and an implementation of Microsoft Office 365 that will be a crucial first step toward all-around efficiency, in a recent article and video by *GovTech*.

Key insights – Artificial Intelligence

CANADA - "To achieve AI prosperity in Canada, it's critical we get public policy right on three key pillars: creating growth in an AI-driven economy, advancing the public good, and building trust in institutions and in society," Deloitte said in a report on AI. Yet only four percent of Canadians surveyed by Deloitte said they were confident in their understanding of AI. According to the report, another obstacle that is stunting growth of AI is Canadians' high level of distrust of the technology.

ESTONIA - Estonia's chief data officer is on a mission to implement AI into every part of the country's public services, from healthcare to education and job centers. Read more about the chief data officer's vision for the future, and early successes thus far.

USA - Overwhelmed by alerts and constrained by limited resources, state government needs a new plan to fight digital threats and attacks. AI could be the answer as it holds promise for sifting through large volumes of security events, increasing the chance that real threats will be detected more quickly. Read more about the defensive capabilities and potential challenges of using AI for cybersecurity at the state level.

UK - On June 10, the UK government announced an investment of up to £18.5 million to support efforts to enhance diversity in AI and data science roles which will go towards conversion degrees, scholarships for under-represented groups and online learning.

Other noteworthy articles on AI:

Independent watchdog key to monitor artificial intelligence, University World News

Other noteworthy articles this month:

Unhappy customers: are inhuman public services destroying trust? The Mandarin

Qld budget sinks $85 million into digital services, cyber security. IT News

Municipal Digital Twins Can Transform City Planning. Forbes

Exclusive: How emerging tech will impact the public sector. IT Brief

Illinois Debuts Portal to Streamline Local Tax Services. Government Technology

Changing the face of local government with digital transformation. Open Access Government

Why Should Your Jurisdiction Have a Facebook Group? Government Technology

Research repository

Access the ICCS Research Repository here.

New content includes: What governments need to be truly citizen-centric; Big Data and Artificial Intelligence — The Future of Accounting and Finance; Ten years on: What's next for behavioural insights?

This month's feature: Personal Privacy or 'Ask Just Once' – Do we have to choose?

In 2017, the Economist declared, "The world's most valuable resource is no longer oil, but data."

Personal data has become big business. According to a 2018 New Yorker article,

> *"We sign up to get [a] service, but we don't give much thought to who might be storing our clicks or what they're doing with our personal information. It is weird, at first, when our devices seem to 'know' where we live or how old we are or what books we like or which brand of toothpaste*

we use. Then we grow to expect this familiarity, and even to like it. It makes the online world seem customized for us, and it cuts down on the time we need to map the route home or order something new to read. The machine anticipates what we want. But … we don't really know who is seeing our data or how they're using it."

In response to the issue of data being used in ways that individuals aren't aware of, some countries have taken a stand to protect a citizen's privacy and personal data.

The GDPR legislation[1] is considered the gold standard in privacy protection. According to the Raconteur, this is because "under GDPR's strict requirements, any business globally that sells to or targets European Union consumers will need to wherever that business is based. The EU is effectively making GDPR a global benchmark for privacy regulation."

The following table[2] provides a quick reference guide to privacy law across some jurisdictions that are also recognized for good service delivery and was built based on data provided by i-Sight and the European Commission, noting that the privacy law in Denmark and UK would be compliant with GDPR:

Country	Canada	Denmark (EU)	Australia	UK (EU)
Sufficient protection according to GDPR?	Yes (commercial organizations - Governed by PIPEDA – see below)	Yes	No	Yes
Privacy Laws	Canada has 28 federal, provincial or territorial statutes governing data protection and privacy in the country. At the national level, the collection, use and disclosure of personal information in the private sector is governed by the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000.	Privacy laws in Denmark are regulated under the Danish Act on Data Protection 2018 Act (Law No. 502 of 23 May 2018), formerly the Danish Act on Processing of Personal Data Law (Act No. 429 of 31 May 2000). This new data protection act supplements and implements the	Australia's Privacy Act 1988 is the key privacy law that governs both the public and private sectors. The Privacy Act is based on 13 APPs (Australian Privacy Principles) that cover transparency and anonymity; the collection, use and disclosure of data; maintaining the quality of data; and the data subject's rights.	The U.K. is currently regulated by the Data Protection Act 2018 which incorporates the EU GDPR and supplements its provisions. The Data Protection Act 2018 focuses significantly on data subject rights, "special category" personal data, data protection fees, data protection offenses, consent

1 General Data Protection Regulation: a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area

2 The countries that were compared were selected because they are deemed to be countries providing excellent digital public sector services.

Country	Canada	Denmark (EU)	Australia	UK (EU)
	PIPEDA was most recently amended in November 2018 to include mandatory data breach notification and record-keeping laws. For the public sector, such as federal departments and Crown Corps., data privacy is governed by the Privacy Act 1983. Provinces and territories each have their own public sector legislation. For example, Alberta is governed by the Personal Information Protection Act (PIPA) 2004. British Columbia is governed by an act under the same name, implemented a year earlier. Ontario also has its own privacy act, the Personal Health Information Protection Act 2004.	General Data Protection Regulation (2016/679). (FYI: EU countries are required to update or enact their own federal privacy acts to match provisions in the GDPR). The Danish Data Protection Act 2018 contains provisions relating to data processing, the disclosure of personal data, the right of access, the designation of a data protection officer, limits on consent, prohibitions on data transfers, administrative penalties and more.	In addition to the Federal Privacy Act 1988, data protection is governed by statutory privacy laws (in the majority of Australian states) and sector-specific privacy laws (depending on the data at hand). For example, organizations that collect, use or disclose health data are governed by separate Health Privacy Principles. Organizations in Queensland that deal with personal data will also be governed by the Information Privacy Act 2009.	from children and enforcement. The U.K. will no longer be an EU member state as of March 29, 2019. However, there has been no word that the U.K. will change its existing data privacy laws.
More information available	• Government Website • PIPEDA 2000 • PIPEDA Amendment 2018 • Privacy Act 1983 • PIPA AB 2004 • PIPA BC 2003 • PHIPA 2004	• Government Website • Danish Act on Data Protection 2018 • General Data Protection Regulation 2016	• Government Website • Federal Privacy Act 1988 • Privacy Principles • Information Privacy Act 2009	• Government Website • Data Protection Act 2018

Privacy is Important: The views of Canadians regarding privacy of personal information

Privacy is important to Canadians

Personal privacy and security have always been important concepts to people in Canada. In Ipsos' Canada Next report (2017), "Three-quarters of Canadians believe that citizens should own data collected on them by governments, and 72% agree that data generated by Canadians should be protected and regulated similarly to a natural resource."

IPSOS also reports that, "69% [of Canadians] agree, that when they think about future advances in technology they are very worried about privacy and the security of their personal information." Canadians also believe that Government data belongs to citizens (see below).

Governments in Canada respect that privacy is important to Canadians

Canadians are satisfied with the way that Canadaian governments respect their privacy, as demonstrated through the feedback provided in the Citizen's First 8 National Report. That report states that, "Government services perform well for the majority of service attributes, including Fairness, Privacy, Communication (being informed of everything you need to do), Outcome and Channel Satisfaction." Participating jurisdictions receive positive scores of 75 out of 100 for Privacy, Communication (being informed of every necessary activity), Outcome, and Channel Satisfaction.

IPSOS also reports that Canadians will share data to support good service

Canadians are expecting more than just respect for privacy. They want providers to make the right decisions around how to continue to support privacy while improving service delivery.

Does it need to be a battleground? Innovation versus protection of information

Traditionally, there has been a tension between the opportunities that information sharing creates for improving the service experience, and protecting the privacy of an individuals' private information. It is a problem that has existed for years, where sharing personal information between organizations and/or jurisdictions facilitates asking individuals for personal information 'just once' for a variety of services. While individuals may want convenience, their interest in providing their personal data once and having it shared across boundaries is not always preferable.

This conflict is communicated in Government Information Sharing: Is Data Going Out of the Silos, Into the Mines? In a 2018 article in Canadian Government Executive, competing positions in the report were identified; that, "all Canadians want the benefits of electronic government services, and reduction of administrative burdens", and that, "some of us still want our privacy and autonomy too."

Herein lies the conundrum for the public sector.

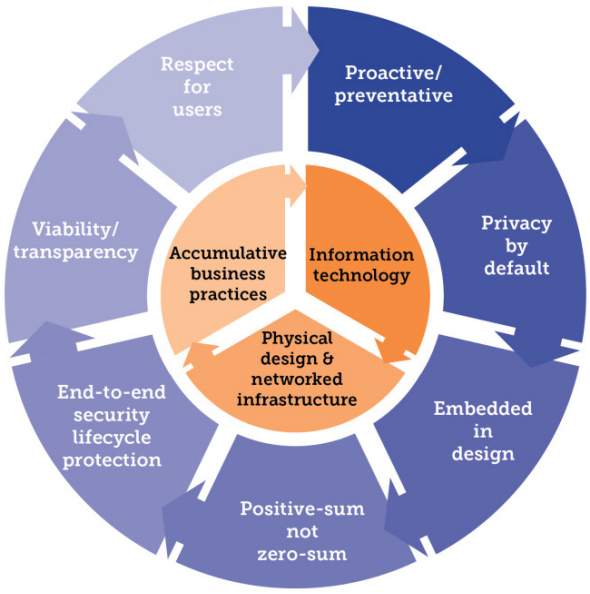
There doesn't need to be a tension. Privacy can and should be built into services as they are designed or redesigned. This is the idea behind the concept of "Privacy by Design".

Privacy by design

Privacy by Design is a specific approach to privacy, championed by the former Privacy and Information Commissioner of Ontario, Canada, Dr Ann Cavoukian, initially in the 1990s but continuing over the subsequent decades. In a Privacy by Design Background Paper, the Victorian Commissioner for Privacy and Data Protection (Australia) describes Privacy by Design as, "a methodology that enables privacy to be 'built in' to the design and architecture of information systems, business processes and networked infrastructure. Privacy by Design aims to ensure that privacy is considered before, at the start of, and throughout the development and implementation of initiatives that involve the collection and handling of personal information."

Dr. Cavoukian explains that, "In this day and age of ubiquitous computing, massive online connectivity [and] social media . . . there's no way we're going to be able to address all of the privacy harms if we don't try and prevent them upfront. You can't just do it with regulatory compliance after the infractions have happened."

The concept of Privacy by Design is based on 7 principles:



The following Cheat Sheet explains these principles. The eHealth system in Estonia, recognized for its work in Digital Government, provides a working example of how Privacy by Design can work. The World Bank summarized this work in its report: Privacy by Design: Current practices in India, Estonia and Austria, as follows:

"User Consent and Choice—eHealth System The core of Estonia eHealth is the Digital Health Record system, using HL7 and DICOM message formats for interconnection. The data transport and security layer are provided for by the "X-Road" middleware software. Patients can view all their health care data through the Estonian eHealth Patient Portal by using their digital ID to authenticate their identity. By default, medical specialists can access data, but any patient can choose to deny access to care providers, including one's own general practitioner/family physician. Others, such as pharmacists and insurance agents, can get access to a patient's medical records, but only with the patient's explicit knowledge and consent. All data access requests within the system are recorded, and patients can on request access this record."

There are further examples of how Privacy by Design works in reality that have been collected by the World Bank in the same report here. Additional resources on the topics are available on the Global Privacy by Design website.

We would love to hear from you!

We would like your feedback!

Please click on the link to answer three simple questions.

Take Survey

Do you know someone who may be interested in the Joint Councils Executive Report? Please share a copy of this report. If you are not already a subscriber, you can now subscribe to receive the Executive Report by signing up here (please scroll to bottom).

Send your questions to info@iccs-isac.org.

Icons made by Prosymbols from www.flaticon.com