THE INTERNET OF THINGS



TIME FOR A NATIONAL DISCOURSE

Release Date: August 2015

ITAC
INFORMATION TECHNOLOGY ASSOCIATION OF CANADA

ACTI
ASSOCIATION CANADIENNE DE LA TECHNOLOGIE DE L'INFORMATION

As Canada's national ICT business association, the Information Technology Association of Canada (ITAC) champions the development of a robust and sustainable digital economy in Canada. A vital connection between business and government, we provide our members with the advocacy, networking and professional development services that help them to thrive nationally and compete globally. A prominent advocate for the expansion of Canada's innovative capacity, ITAC encourages technology adoption to capitalize on productivity and performance opportunities across all sectors. A member-driven not-for-profit, ITAC has served as the authoritative national voice of the $150 billion ICT industry for 60 years. More than 33,500 Canadian ICT firms create and supply goods and services that contribute to a more productive, competitive, and innovative society. The ICT sector generates one million jobs directly and indirectly and invests $4.8 billion annually in R&D, more than any other private sector performer.

On June 16, 2015 the Information Technology Association of Canada (ITAC) set out the association's thinking on the internet of things (IoT) as part of an investigation into 'disruptive technologies' being conducted by the Standing Committee on Industry, Science and Technology of the House of Commons.

ITAC called for a national discourse on the benefits and challenges related to the rollout of the IoT across Canada and around the world. This ITAC white paper, already underway at the time and referred to in the Committee presentation, discusses this coming wave, the public policy environment and the need for further investigation, and highlights the opportunity for Canada to establish itself as a leader in the evolution of the IoT.

1. THE COMING WAVE

The following are just three examples (all drawn from the ranks of ITAC Ingenious Award winners) of Canadian organisations reaping early benefits from a suite of technologies that combine to create the Internet of Things.

- A small company from Airdrie Alberta, Growsafe, has pioneered the use of radio frequency identification tags in livestock. These tags, combined with an array of sensors, can measure a multiplicity of factors relating to the well-being of a farm animal. These factors include feed and water consumption, daily body weight and environmental factors, such as humidity and wind speed. In one small feed lot, for example, Growsafe can collect more than 70 million data points a day and analyze that data in milliseconds. This gives farmers new visibility on the growth, health and development of their animals. Based on this, Growsafe's behaviour patterning can identify a sick animal and send the appropriate care alerts more than four days before symptoms appear. Growsafe can also help farmers reduce an animal's feed intake and even lower methane production, ensuring healthier animals enter our food system.

- Dr Carolyn McGregor, Canada Research Chair in Health Informatics at the University of Ontario's Institute of Technology, leads a project that is significantly improving the survival of premature babies. By combining cloud computing, wireless technology and big data analytics, Dr McGregor's Artemis project team has created a platform capable of processing 1200 physiological readings per patient per second across multiple patients in multiple locations. The Artemis team has already demonstrated new earlier detection approaches to Late Onset Neonatal Sepsis, a dangerous infection common in preemies.

- In its Chelopech gold mine in Bulgaria, Dundee Precious Metals uses a WiFi-based tracking and production system (the first of its kind in the world) to monitor the safety of its miners and the efficiency of its operation. Dundee utilizes a 3-D tracking system to acquire real-time visibility into their entire underground operation, including the movement of ore along the conveyor belt and the current location of individual miners.

The system also monitors the status of each piece of equipment and can schedule preventive maintenance before an outage occurs.

The Internet of Things (IoT) has been defined as a network of networks of uniquely identifiable end points or things that communicate without human interaction using internet protocol connectivity – though other protocols, such as RF (radio frequency) and Bluetooth, are also part of the picture. The IoT is a capability rather than a technology, a complex convergence of the various technologies and services that make up the ICT sector. These include computer and telecom hardware, equipment and services, software, semiconductors, sensors, big data / analytics, applications development, mobile platforms, security and wireless technologies. Put simply, sensors with embedded intelligence enhance the power of the network by collecting and reporting data from their environment that is compiled and analysed to generate information about context.

The transformational potential of the IoT is such that proper and measured application will greatly improve the lives of Canadians by, for example:

- improving safety and security at home and in the workplace
- improving access to remote healthcare service
- enabling innovative solutions for environmental and other pressing public-policy issues.

The roll-out of the IoT will also dramatically improve Canada's economy by helping our companies become more competitive. After all, the IoT was envisaged as solving specific business problems in critical business verticals and functions. Canada as a whole will be benefit from its positive effects on the operations of companies large and small – virtually all of which will see ways to take advantage of IoT-based capabilities.

The IoT is the next 'natural' wave of connected devices, after the internet of fixed devices (laptops, desktops) and internet of mobile devices. It also builds on the following key drivers: connectivity and network evolution, sensors and microprocessor design and cost, big data and analytics, cloud-computing technologies and mobile business applications.

In 2008, the year that the global number of internet connected devices first outnumbered the human population, the US National Intelligence Council declared that the IoT would be a disruptive technology by 2025. Since then, that estimate has been revised forward; Gartner estimates that there are over 3.8 billion connected things on the planet today and that by 2020 that number will climb to 25 billion. At that point, IoT devices will be generating $8 trillion in annual revenues. Apart from its sheer size, this economic activity will touch virtually every human on the planet. In Canada, IDC predicts 21% market growth (i.e., revenue) from 2013-2017; IDC also predicts that the IoT will be a $21 billion market in Canada by 2018.

This wave will disrupt established business models and it will bring consequences, both positive and negative, that should concern Canadian public-policy makers. Fortunately, Canada has an excellent track record in its comprehension of the importance of connectedness in the ongoing task of nation-building. Philosophers from Innes to McLuhan have demonstrated how Canada is fundamentally an expression of the will of its people to connect with one another cross vast distances. Policy makers have recognized this as well. The Information Highway Advisory Council (IHAC) launched a nation-wide conversation on the internet that helped to establish many of the principles currently governing our connectedness. Canadian policy makers were also in the forefront of the OECD's efforts to understand and seize the economic benefits of the internet. This legacy alone makes the quest for a deeper understanding of the internet of things important. The range and impact of the public policy implications surrounding it make this imperative.

2. THE PUBLIC POLICY ENVIRONMENT

ITAC, the voice of the information and communication technology industry in Canada, looks at public policy through the filter of technology. The inventory of public policy issues raised by the IoT that we have listed below is not comprehensive, yet it is lengthy and these issues will have an impact on every Canadian. Together they represent what we believe is a strong case for a national conversation that will produce, in a strategic and methodical way, the public policies necessary to ensure Canada's continued leadership in the connected world as well as the prosperity and well-being of its citizens for generations to come.

While the IoT will be disruptive, it will be an evolving phenomenon and is very much the extension of the current use of technology. Canadian companies see the intrinsic opportunities and many have invested heavily in building the capacity needed to provide IoT services. This raises key policy questions and while many of our existing policies will be robust enough to handle the evolving IoT context, some may require modification. A comprehensive national discourse on IoT would help to identify gaps and ensure Canada is positioned for leadership in this area.

Among the key issues are privacy, healthcare, a connected world, security, and bandwidth and network capacity – though other issues must be acknowledged and taken into consideration as well.

2.1 Privacy

One of the greatest concerns raised by the emergence of the internet was the threat it posed to privacy. Canada is at the forefront of global leadership to safeguard privacy. Privacy by Design, a concept introduced by Ann Cavoukian, Executive Director of the Institute of Privacy and Big Data at Canada's Ryerson University, provides the framework needed to ensure that the privacy rights of individuals are addressed in the design and deployment of IoT networks and devices. Canada also has a comprehensive legal framework in place to protect privacy with laws in place

at the federal, provincial and territorial levels. As recently as June 2015 the importance of privacy was reiterated by the Office of the Privacy Commissioner: "Uncertainty as to whether privacy is being adequately protected would have the effect of undermining trust in Canada's technology sector as well as stifling business opportunities and innovation. It could also erode commerce and trade and hamper Canada's ability to compete on the global marketplace. It would be in all our interests to ensure that Canada's privacy protections remain relevant in the face of new and complex threats."

The IoT and other technological trends such as cloud computing, mobile apps and Big Data analytics are raising new questions about the privacy of personal information and the ability of individuals to control the collection, use and disclosure of information about them. We need to redefine privacy in the digital age. This evolution demands an active discourse on how we maintain the privacy rights of individuals while at the same time reaping the benefits of the digital age. This discourse was challenging enough when connectivity was limited to computers and networks. In light of the forecasted expansion of IoT applications, and the exponential increase in associated data volumes, it is about to get dramatically more complex. (IDC estimates that the volume of data generated on a global basis will grow to 44.4 zettabytes.)

2.2 Healthcare

The fusion of mobile communication with analytic tools has been a great asset to people living with chronic health problems. In 2013, a Pew Institute study found that 21% of Americans were using technology such as glucometers and telemetric blood pressure gauges to monitor their conditions.

In Canada, it is estimated by IDC Canada that $1 billion will be spent on technology for the healthcare sector in 2013. Machine-to-machine (M2M) technology, a significant subset of the IoT, is expected to represent the majority of this investment. Telehealth saved more than 47 million kilometres in travel and $70 million in personal travel costs for patients and their families in 2010 alone, according to Canada Health Infoway, and savings can be expected to increase dramatically in coming years.

Monitoring health data with technological devices appears to be even more pervasive among the healthy. The 'quantified self' or 'self-tracking' movement has created a tremendous demand for devices like Fitbit Trackers that record key fitness performance metrics. Some analysts expect this market will expand to nearly half a billion devices shipped annually by 2018. This will produce an explosion of personal data that is vulnerable to misuse. The dilemma is put succinctly in a recent study by Symantec: "Ultimately the more data we collect and store about ourselves, the more opportunity there is for us to learn about ourselves, but it also opens up the opportunity for others to learn the same about us."

At the same time, one of the barriers for consumers adopting these new technologies is concern over the privacy and security of the data. They wonder who is collecting it and who are they selling it to, especially when it involves sensitive matters like healthcare.

2.3 A Connected World

Very soon the amount of personal data we collect will be augmented by what the machines and the things around us know. Smart cars will not only be able to drive and park themselves, they will be able to pinpoint our locations. With the advent of IoT-driven household appliances, our consumption patterns will be collectable and transmittable in real time. While much of the data generated by the IoT will be completely non-personal in nature, it is no overstatement to suggest that the IoT has the potential to transform the nature of the private citizen. Policy makers need to consider the impact that the IoT will have on things like automobile and home insurance, licencing and taxation.

With recent amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), data breaches in Canada must now be reported. Nevertheless, more may need to be done to ensure that public policy on this issue is not completely outpaced by technology. This is not just a question for Canada or any other individual country; it is an area of public policy that demands international approaches so that, for example, countries have the same breach-notification rules and respect and work to support each other's enforcement actions.

2.4 Security

Security concerns related to the IoT include data collection, encryption, transmission and storage, malicious attacks, information privacy and BYOD (bring your own devices). A recent report the President of the United States from the National Security Telecommunications Advisory Committee (NSTAC) observed:

> The IoT will bring significant societal benefits, many of which are already being recognized through increased efficiencies, early detection of faults, improved reliability and resilience and more. But the rapid and massive connection of these devices also brings with it risks, including new attack vectors, new vulnerabilities and, perhaps most concerning of all, a vastly increased ability to use remote access to cause physical destruction.

One of the most frequently cited illustrations of this are patients on internet connected devices such as insulin pumps or pacemakers. These devices will be very effective at managing a patient's health condition. However, hacked by a malicious actor, they will also be able to deliver a fatal overdose or electrical charges.

As the NSTAC report notes, IoT exponentially expands the number of 'attack surfaces' that maliciousness may target. It doesn't take a great leap of imagination to realise that if the IoT permits you to control your home furnace remotely, then a hacker who wishes to harm you may interfere with your controls. Interconnected cities and transport systems and the machinery and things that operate them must be secure against such malicious attacks. The scale of possible attack, remotely initiated from a device virtually anywhere in the world, is sobering, and

it is a trivial matter to attack and compromise many of the sensors currently in use. This is and will continue to be a real barrier to adoption once the first major data or system breach occurs until all devices and services offer strong security protections.

2.5 Bandwidth and Network Capacity

The networks that make the Internet of Things possible rely on scarce resources that require careful public stewardship – spectrum and internet addresses. Already telecommunication industry leaders are speculating that the IoT will have a profound impact on our communications networks, eventually increasing data volumes on our networks one thousand-fold. Canada's telecom carriers are investing heavily in their networks to accommodate the anticipated growth in data traffic in Canada, which Cisco projects will triple by 2019.

Volume will not be the only force straining the networks. Cisco also projects that there will be 382.4 million networked devices in Canada in 2019 (more than 10 per person on average), up from 185 million in 2014. The diversity of the devices interacting with communication networks will demand they become vastly more complex. As Ericsson Canada President Mark Henderson warned at a recent Canadian Telecom Summit, “Traditional networks and their one-size-fits-all approach needs to be adapted to the thousands of use cases and the many different subscriber types (the IoT will bring).”

The ICT industry must come to grips with this of course, but industry is not the only player in network development. Spectrum is a natural resource that will increase in value as it decreases in availability. The task of spectrum allocation, making wise decisions to extend the benefits of the IoT as widely as possible, will, like the networks themselves, become more complex. However, with that anticipated arrival of multiplexing technologies that will enable the attainment of very high speeds by carrying and merging data streams across several different spectrums, regulation may not be necessary.

This complexity extends even into network governance. At present the view that “a bit is a bit is a bit” is pervasive and foundational to net-neutrality approaches to governance. On a network where a bit may carry a lifesaving drug dosage or the means to avert a terrorist attack as well as twitter feeds and video downloads, our governance protocol may require rethinking in exceptional cases where bottlenecks in the networks exist, typically rural and remote areas. This flies in the face of concerns around network neutrality, but we believe it is at least worth of discussion.

Spectrum isn’t the only scare resource. The world is rapidly running through its supply of internet protocol addresses. IPv6, the most recent version of internet protocol that provides an identification and location system for the internet, holds the promise to replenish this supply.

2.6 Other Issues

Additionally, there is a broad array of economic and commercial public policy issues engendered by the IoT.

2.6.1 Ownership of Intellectual Property and Data

Ownership of intellectual property and data is one issue. Apart from the ever more challenging issues regarding classically defined IP in a world where everyone and everything is connected, the IoT expands concerns around who owns the data being generated and collected. If the answer is the individual generating the data, how do they acquire the means to defend their rights against infringement that may come from anywhere in the world? The monetisation of data generated and captured through IoT interactions will drive many business models yet to be created, so data ownership needs to be clearly defined by countries and regions.

2.6.2 Standards Development

Another issue is the development of standards. Concerted international efforts are required to develop a comprehensive suite of robust international standards that will ensure the interoperability of devices around the world. If we want our Korean-built device to communicate with our Mexican-built device, then they will have to be programmed to understand a common 'language'. And if we travel from Canada to Korea, then we will want the local networks and devices to be able to interact effectively with whatever personal and corporate devices we've brought with us. Even if it is true that the consumer doesn't care about interoperability, that is because they assume it – and industry must and will see it as an absolute commercial requirement. Canada and Canadian companies need to continue to play active roles in international initiatives currently under way at the ISO, the ITU and the M2M World Alliance. The work being done by these and other groups are key elements in the development of an effective IoT, and should be supported by Canada's government agencies.

2.6.3 Trade Agreements

Because of the global nature of 21st century connectivity, the legal frameworks governing IP and standards will also feature prominently in trade agreements. Recent Canadian trade agreements have demonstrated a high degree of digital literacy and an understanding of the electronic nature of modern commerce. This must continue to be enriched to meet the challenges of a global IoT. Trade agreements should also incorporate ambitious digital-trade provisions, specifically those that would enable cross-border data flows and limit the imposition of restrictive measures regarding the location of cloud-computing and storage infrastructure.

2.6.4 Workforce

There will be workforce implications stemming from the Internet of Things. It will inevitably disrupt business models and create new opportunities. The challenge for policy makers will be to mitigate the former and maximize the latter. To do this effectively will require a sound understanding of the national digital labour force (now comprising about one million Canadians) and effective partnerships between employers, academe and government to ensure it is globally competitive in the future.

2.6.5 Network Infrastructure

An inevitable component of the advent of the IoT will be the development and installation of much more network infrastructure across Canada and globally, and the government should see telecom networks in the same way as they do buildings and bridges, the design, construction and management of which is overseen by qualified professionals. Canada currently lacks sufficient skills in network design and installation, and with only a handful of educational institutions offering engineering programs with specialisations in networking it is difficult to see how the need for skills will be filled.

3. CONCLUDING REMARKS

Our stewardship of Canada's role in the Internet of Things must also be as cognizant of the opportunities inherent in the IoT as we are about its challenges. One very clear opportunity is to build upon Canada's tremendous legacy of expertise in the art of connectedness to establish our nation as a leader in the evolution of an Internet of Things that delivers value to all Canadians.

Canada can be a leader in the IoT. ITAC believes we must aspire to do so and to build a pathway toward this leadership. This will require sharing information, meeting the challenges of the IoT head on and above all engaging all stakeholders in a national conversation about the next evolution of the internet. ITAC strongly recommends that government initiate this discourse as soon as possible. As the previously cited NSTAC report notes, time is of the essence. "There is a small – and rapidly closing – window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations."

For our part, ITAC and the IoT roundtable that we have created has pledged to contribute and provide the perspective, insight and knowledge of Canada's ICT industry to this important discourse.