HERJAVEC GROUP

Statements from the

Canadian House of Commons Standing Committee on Access to Information, Privacy, and Ethics

February 28, 2019

Statement by Ira Goldstein, Herjavec Group

Good afternoon and thank you to the chair, the vice-chairs and the members of the Committee for the opportunity to speak today.

My name is Ira Goldstein. I am the Senior Vice President of Corporate Development at Herjavec Group. I have spent the last decade working in Information Security to help companies and governments secure their most critical digital assets. I am joined by Matt Anthony, Vice President of Security Remediation Services at Herjavec Group, whose remarks will follow.

Herjavec Group was founded in 2003 by Robert Herjavec, who emigrated to Canada with his parents from Eastern Europe. A dynamic entrepreneur, Robert has built Herjavec Group to be one of the largest privately-held cybersecurity firms in the world. Our experience includes working with private and public sector organizations in complex, multi-technology environments to ensure their data security and privacy.

We are honored to address the Committee today on behalf of Robert, Herjavec Group and our fellow Canadians.

Our statement will address two subject areas related to the Committee's study. First, I will outline why Digital Identity is a key building block in the transformation of Government Services. I will then outline steps to manage, govern and secure our digital identities. My recommendation is for the Government to tread lightly on the broader transformation path to ensure privacy and security are top priorities. In parallel, the Government should move quickly on a pilot project to expand existing success in Canada's digital presence.

Digital Government Services must be built on a foundation of Identity good-governance. If our identities are to be digitized and managed by Government, citizens expect a system that

ensures security and privacy. Our identity attributes are assumed to be protected by the issuer, our Federal Government. In any system, physical or digital, fraud is a risk that must be mitigated through effective controls and ongoing assessment.

These concepts are not far from realization. When a baby is born or a new immigrant arrives, individuals may request their identity documentation online. Ultimately, physical artifacts are issued as proof of identity. But the fact that we have an online portal to provision identification means that we have the foundation to leverage that data for use in a digital government service.

Several Government services are already online. One of the most critical functions of Government, tax collection, is digitized through Canada Revenue Agency's eFile system. Presumably, the push to eFile was supported by

efficiency outcomes, and stands as a successful case study of digital transformation.

Any further steps to digitize citizen identity must consider the perception of an impact on individual privacy. Individuals may perceive digital identity as a threat to privacy, despite the expected benefits. One recent example is the speed at which public perception soured over Statistics Canada's plan to collect personal financial information. Despite involvement of the Privacy Commissioner and plans to anonymize the data, perception quickly turned negative towards this prospect.

The contrast between CRA's eFile success and StatsCan's attempt to gather financial information is a guiding light for the Committee. Digitizing Government services will be welcomed by the Public if managed and messaged thoughtfully. The upside to this effort is more access for historically marginalized groups and geographies, so the opportunity cannot be ignored.

Historically, identity proofing has required a trusted, centralized authority to govern provisioning and usage. If I want to prove who I am, I need to show Government-issued Identification. I foresee this authoritative proof as a permanent feature of modern democracy, so despite the advances in decentralized identity, the Government has an important role to play in Identity Management.

In sum, I strongly recommend the Committee seizes the opportunity to further digitize components of citizen Identity to enable the efficient and secure delivery of Government Services, while taking caution in the line we must draw between centralizing data and ensuring that individual privacy is maintained.

Statement by Matt Anthony, Herjavec Group

Good afternoon. My name is Matt Anthony, Vice President of Security Remediation Services at Herjavec Group. I have worked in information security in public and private sector for more than 20 years. I'm honored to be here today to address the Committee. I'll keep my remarks focused on two main areas of concern.

Firstly, I would like to address the issue of e-government – specifically the pace and volume of change. There have been great successes, from tax filing to pet registrations, at all levels of government.

Fear-of-missing-out and reputation-enhancement are drivers of many initiatives and can influence the adoption and adaptation to e-government. Facebook founder Mark Zuckerberg famously said: "move fast and break things", and that became the mantra of developers around the globe. While moving fast and breaking things might be an essential business model in some cases, Government does not – or should not – have that luxury. Herjavec Group's Cyber Incident Response teams have seen the direct impact. Breaches are large, costly, and damaging.

There is a dramatic global skills shortage in the core capabilities needed to securely govern, develop, test, deploy, and maintain complex software systems. Current published figures estimate that there will be 3.5 million cybersecurity job openings worldwide by 2021. The global digital transformation is in direct tension with this; more projects, more services, more data: created, stored, managed, shared, and mined. Canada, and Canadian governments, will feel this tension acutely.

The Committee has heard a great deal about three case studies: Sidewalk Toronto; Estonia, and Australia. I'll address the Estonia case briefly.

Estonia had many advantages in digital transformation that Canada does not have: a small population, a small geography, a relatively green field in the post-Soviet era, and a relatively homogenous population accustomed to central control. Take away these advantages, and the model may look very different. While the transformation appears successful, we don't know a lot about the security and privacy protections or robustness. I caution against using it as a north star.

You cannot stand still, but my hope is that we go slowly enough to be assured that any changes can be fully governed and secured to the appropriate level. Go carefully according to strong principles. Wait when necessary for technologies such as AI and automation to support us better. Do not allow FOMO and international comparisons to cause us to hurry ahead of our abilities and capabilities.

Secondly, I would like to briefly address Information Sharing.

I want to commend the Data Strategy Roadmap. The six "most important things" are concise and precisely correct. I cannot, in this short time, do much better than to amplify them. The concepts are simple; develop a strategy; provide clarity on data stewardship; develop standards and guidelines for governance; improve recruitment to gather the needed skills; and develop technology systems that support the Strategy. Each of those is enormously difficult to do in practice.

In 1984, Stewart Brand presciently wrote "Information wants to be free". This related to the constantly lowering of cost of sharing. Now, it has become synonymous with the relatively difficult problem of keeping access control; once information is beyond the source's control it will tend to get distributed. It follows that secondary and tertiary use of public data needs to be as astutely controlled as primary use.

The Government faces a monumental task in understanding and managing legacy data and systems. Reconciling inconsistent or undocumented: consents for use, information silos, usage rules, data structures, identity platform and administrative processes will be monumental in scale.

I believe taking a greenfield approach may be advantageous – establishing rules clearly for new data collection and allowing legacy data to be integrated in the future as capabilities such as AI data tagging and collection management can be paired with lower costs for transformation through automation. Don't rush to the data lake model, as unexpected de-anonymization and information correlations will emerge, some of which may be contrary to public policy, law, or intent.

There are a lot of assertions that "opportunities" will emerge and "efficiencies" will be achieved by aggressively mining, aggregating, and sharing data. Require evidence to show that.

As advice to the Committee, I urge the Government and Industry to slow down, be more careful, and do not allow ambition to overshadow capability. Go slowly enough to fully understand, measure and manage information risks. Criminals like data. Breaches are messy, complicated, and very expensive.

About Herjavec Group

Dynamic entrepreneur Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. Our service expertise includes Advisory Services, Technology Architecture & Implementation, Identity Services, Managed Security Services, Threat Management and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom and Canada. For more information, visit www.herjavecgroup.com.

Follow Us

Herjavec Group
@HerjavecGroup