Kalev Leetaru, contributor

This past Friday the World Bank hosted an all-day conference titled "Estonia ICT Day: Smart Digital Solutions for Sustainable Development" at its headquarters here in Washington, DC that I was honored to attend in person. With presentations by Estonian President Toomas Hendrik Ilves, Director General of the Information System Authority of Estonia Taimar Peterkop, and many other luminaries, the day focused on how Estonia has become the global model for e-government with almost every task from voting to filing taxes to purchasing a fishing license accomplishable entirely online. In fact, today one need appear in person at a government office only to finalize marriage or divorce and to purchase property – every other transaction between a citizen and the state is completed entirely online and can be done via smartphone from anywhere in the nation or even abroad.

The day's opening keynote address was provided by President Ilves, who offered a summary of how Estonia rebuilt itself after its 1991 independence by focusing on the technology sector. A central tenant of that redevelopment involved employing technology, automation, and the nascent web to build an e-government that would leverage computerization of traditionally time-consuming paper processes to allow a relatively small government to provide a level of service on par with vastly larger and richer nations.

In this vein, he noted that automation is often viewed with fear in many countries, that technology will displace jobs and raise unemployment. In the case of smaller nations like Estonia, however, he said that precisely the opposite is true – such automation allows a relatively small workforce to be far more efficient and to accomplish what traditionally would require a vastly larger team with a much larger budget.

For example, the size of the national tax collection authority shrunk by nearly half after the introduction of electronic tax filing, while providing the same level of service. This allows smaller countries like Estonia to accomplish far more per employee and per dollar spent, serving their citizens in a much better way.

Underlying the Estonian e-governance model is a fully decentralized data fabric premised on a model of "only once" in which any given piece of information about a citizen is requested only a

single time and held only by the agency requiring it. Thus, instead of the US model, where you must repeatedly provide your name, address, social security number, and other details in practically every encounter with the US Government and often repeatedly in the same paperwork in the same visit, the Estonian model requests this information just once and keeps all of it separate, linking it transparently and only as needed.

From a citizen standpoint this absolutely minimizes the amount of information that one is required to provide in a given encounter with the government, ensuring that every transaction is as streamlined and rapid as possible. Mr. Peterkop gave the example that a citizen could be walking along a river in a forest in rural Estonia, decide suddenly that he wanted to go fishing, and simply pull out his smartphone and purchase the necessary fishing license in less than five minutes while standing in the middle of the river with his fishing rod ready to go (in fact 90% of fishing permits are issued online). Almost a third of votes were cast online as of last year.

In a nod to nations like Greece that are struggling with tax revenue collection, President Ilves noted that when tax filing was made available online, compliance rates increased due to the streamlined process, taking less than five minutes on average to file a tax return and with refunds issued in less than a week.

Such a model lies in contrast to that of many other nations like the US Government, which suffer from heavy duplication of data across agencies and databases due to their historical legacy of paper records that required such duplication. Yet, most intriguingly, in today's world of heightened cyber vigilance one of the most common refrains of advice for governments and corporations alike is to centralize their most sensitive and precious records into a small set of heavily protected data stores. This has the advantage in allowing all resources to be focused on protecting a relatively small number of high-value cybersecurity targets. On the other hand, this also means that attackers can focus all of their efforts on just a single target and even the most hardened of data stores will always have a weak link. The US Office of Personnel Management discovered this the hard way earlier this year when a single breach was able to disclose a massive cross-section of the US Government's most sensitive personnel records.

Instead, by decentralizing records across the government and with each agency holding only a tiny piece of the overall data environment, the Estonian data model has no single points of failure and a successful breach would compromise a very limited amount of information.

When asked how Estonia chose this model and what kind of roadmap other countries should

follow to build a system similar to Estonia's, President Ilves noted that the decentralized model actually happened by accident. At the time Estonia was building its first e-governance platforms most other nations were building massive centralized data centers using huge mainframe supercomputers. Estonia couldn't afford to purchase or maintain such massive technology investments for its government services so it had to be innovative and piece together a distributed fault-tolerant environment by cobbling together a dispersed cluster of comparatively commodity systems. Over time it became clear that such a model had considerable benefits over the centralized mainframe model and became an integral part of Estonia's long-term e-government strategy.

In fact, today Estonia spends just $63 million a year on IT government-wide, compared with the nearly $700 million the US allocated to Healthcare.gov alone.

The President noted that the system's decentralized nature makes it far more resilient to sustained cyber-attacks, an important consideration for the first country to endure a nation-wide cyber-attack. To bolster this, Estonia has developed the concept of "data embassies" that are essentially remote backups of the entire records of government stored in set of data centers around the world, ensuring that even if a massive calamity were to damage or destroy government facilities in the homeland, the nation would continue to survive with all of its records intact. Estonia, like most countries, has specific laws requiring that government records reside exclusively on national territory for national security purposes. Making use of the Vienna Convention protections that grant "sovereign soil" status to embassies, the President noted these remote backup facilities are located within Estonian embassies in a set of countries around the world, meaning since they are within the embassy grounds they are still formally on Estonian soil, but with the benefit of geographically distributing the doomsday archive of the nation. He noted that such a model might be especially useful to nations in seismically or climatically active regions.

As for a roadmap that other countries could follow, President Ilves noted that, in true agile development fashion, Estonia's e-government systems have been built iteratively over many years, focusing piece-by-piece on the nation's evolving needs. Thus, he emphasized that there is no single "master plan" document that other countries could follow step-by-step to replicate its success. However, Estonia has licensed its entire software infrastructure openly and partnered with the private sector to commercialize and redistribute the system to other governments around the world, with a number of other countries adopting or evaluating the technology already. This allows nations to "drop in" Estonia's innovations either piece-by-piece or as an entire digital government in a box.

In fact, United States Deputy Chief Technology Officer Ryan Panchadsaram noted that the United States had met with Estonian e-government representatives and was closely examining Estonia's system as a model for the US Government.

President Ilves noted that a founding tenant of Estonia's e-government infrastructure is the concept of transparency – that every citizen has the right to see not only all of the data that the government holds on them, but a complete list of everyone who has ever accessed those records. In fact, at any time an Estonian citizen can access a secure dashboard listing the complete history of all accesses to any data held on them by the government. In contrast, in United States citizens have no legal right to demand a master inventory of every record held about them by any government agency or to request a master log of every access to any of those records (and few agencies even have the infrastructure in place to log every access to an agency record).

Putting this into perspective, even the Chairman of the United States House of Representatives Oversight Committee had no ability to know that at least 45 Secret Service employees accessed his personnel record and widely distributed it, including to the Washington Post after a highly contentious hearing involving the agency. Thus, in the United States even a senior lawmaker has no visibility into government access of his records, while in Estonia every single citizen has total visibility and control over their data.

It was noted that Estonia is rated by Transparency International as the least corrupt of all former Soviet Republics and in 2014 it was ranked the 26th least corrupt nation on earth. The President attributed this in large part to digital government's natural resistance to the kind of bribery and favoritism that enables and promotes corruption, quipping "you can't bribe a computer." In fact, the President noted that the anti-corruption effect of digital services has actually been viewed negatively by some countries in which corruption is a central part of doing business, suggesting strong potential for automation to root out endemic corruption. The notion of using algorithms to objectively oversee routine governmental transactions like tax collection, licensing, and other activities that are frequent bastions of corruption is a fascinating concept and one that holds tremendous promise for countries trying to shake off legacies of corruption.

One final question the President was asked revolved around how Estonia came to have free wifi internet access across the country, which has become one of its trademarks. He noted that this was in fact a product of capitalism rather than government intervention. A handful of cafes in the tourist area of Old Town in the city of Tallinn had decided to offer free wifi to patrons in a bid to attract customers wishing to check their email and catch up the latest events. In turn, the other cafes had to offer their own free wifi to compete, which in turn led to other businesses like hotels

having to add the service until eventually it had spread across the country.

Through necessity and built via an agile development process, Estonia has become an unexpected global model for the future of e-government, today offering nearly every governmental interaction with its citizens online. Even the United States has turned to Estonia in its own efforts to try and modernize America and bring its governmental systems into the twenty-first century. With this digital revolution has come increased transparency and compliance, decreased waste and corruption, and an economic powerhouse that has rapidly built the nation into a digital-first workforce and stands testament to the power of data and technology in making government work for its citizens.

Original article on the Forbes webpage .