The Right Mix: How Estonia Ensures Privacy and Access to E-Services In The Digital Age

By: Eric Jackson

For the first time in history every nation in the world operates in an online capacity (UNDP E-Governance Survey, 2014). As governments seek greater efficiency and innovative solutions for citizens, they are increasingly embracing online services, or "e-services," such as tax declarations, medical insurance, permits, prescription databases, and hundreds more. However, what this requires, is government being able to access sensitive personal information. Fear of Big Brother is not anything new, but in an era of unprecedented connectivity and ease of online surveillance, fears are justly amplified. So the problem becomes: how does a government provide quality, comprehensive e-services on one hand, but on the other, ensure citizen information is protected and not misused for illicit purposes? The solution comes from the Republic of Estonia.

This Baltic nation of 1.3 million people may be small in population, but they have big ideas on how the government to citizen relationship (G2C) should work. Historically, Estonia lived under Soviet occupation for half a century. Based on this unfortunate period, the Estonian leadership understands that in order to implement e-services and have the population actively use them, trust must be built and maintained between the public sector and citizens.

Thus, Estonia created an accountable and accessible e-service environment by coordinating three areas: clear and established legal parameters for personal information privacy, an independent enforcement mechanism for these parameters, and lastly, one of the highest internet penetration rates in the world. These factors contribute to Estonia ranking 15th for e-governance implementation out of 193 countries (UNDP E-Governance Survey, 2014) and 28th out of 177 countries for transparency. For nations in the infancy stages of creating e-service platforms, Estonia provides a model for nations looking to expand e-governance, or at the very least, a source of framework ideas to take into consideration.

Estonian personal data protection originates from the 1996 Personal Data Protection Act (PDPA), which was most recently updated in 2008. Although the PDPA has adapted over time to reflect changing technologies and practice, one central component has remained the same: consent. Sensitive personal information (biometric, ethnicity, sex life, trade union membership, state of health, for example) can only be opened by a government agency if the subject willfully consents to its usage. To elaborate further, the PDPA does not consider "silence or inactivity" consent, and gives citizens the right to make consent "partial and conditional" (§12.1). By expanding the concept of consent, Estonian citizens are protected against their personal information being processed without permission. It also lets citizens flexibly choose which e-service fits their needs most.

To access e-services, an Estonian citizen uses their government issued ID card with a microchip containing encrypted personal information. This ID card is then inserted into an inexpensive card reader via computer (e-ID), or using mobile-ID (m-ID), a citizen can log in by smart phone. After this is completed, the citizen can choose from hundreds of e-services through the state online portal Eesti.ee.

When an Estonian citizen does consent to use of his or her personal information, there are seven important legal principles laid out in the PDPA a data processor must follow (§ 6.1-7):

1) **Principle of Legality** - The personal data of an individual will only be collected in an honest and legal manner.

2) **Principle of Purposefulness** - Personal data will only be collected for achieving determined and lawful objectives, and will not be processed in a manner not conforming to objectives of data processing.
3) **Principle of Minimalism** - Personal data will only be collected to the extent necessary for achieving determined purposes.
4) **Principle of Restricted Use** - Personal data will be used for other purposes only with the consent of the data subject or with the permission of the competent authority.
5) **Principle of High Quality of Data** - Personal data will be up-to-date, complete and necessary for the achievement of the purpose of data processing.
6) **Principle of Security** - Security measures will be applied in order to protect personal data from involuntary or unauthorized processing, disclosure or destruction.
7) **Principle of Individual Participation** - The data subject will be notified of data collected concerning him or her. Furthermore, the data subject will be granted access to data concerning him or her and the data subject has the right to demand the correction of inaccurate or misleading data.

Under these seven principles, data processors are legally obligated to follow proportionality; the means used to collect and process data have to be in proportion to the end objective. If a citizen submits personal financial data for tax declaration, that information can only be processed by the Estonian Tax and Custom Board and only used for that specific purpose. Additionally, every data processors is aware of the fact that a citizen from a home computer or mobile phone can observe if there was unlawful access to their personal information. By logging in with e-ID or m-ID, an Estonian citizen can see who is accessing their personal information and what kind of personal information is being accessed. They can even prohibit third parties from using their data for consumer habit research and direct marketing.

Ultimately, it is the citizen who controls his or hers information; not the government institution sponsoring the e-service. Therefore, the relationship between processor-citizen (or government agency to citizen) has built-in transparency, and when there is transparency, there is a greater amount of trust in the system. But as always, the success of legislation is contingent upon how well it is enforced. This is where an integral organization, the Data Protection Inspectorate, assumes a critical role.

As an independent and multifunctional organization, the Data Protection Inspectorate (DPI) provides legal enforcement for upholding a citizen's right to data privacy. For instance, the DPI is both an ombudsman and preliminary court. This means it has the power to make legally binding decisions on whether the PDPA has been violated. It also serves as an outlet for citizens to voice their concerns about the nature of access to their information. In the area of transparency, the DPI can do on-site auditing of public sector institutions, and apply misdemeanor fines or even file criminal charges if there is illegal access of citizen data. What the DPI ensures is citizens have a legitimate and impartial outlet to lodge formal complaints against public sector institutions who are not upholding Estonia's PDPA. Most nations in the E.U. with data protection laws also have a quasi-independent ombudsman, but the actual enforcement of these laws varies between countries, especially former republics of the Soviet Union.

Based on data, the DPI empowers citizens in the government to citizen relationship: in 2013, the DPI processed 1,370 requests for explanations and information, while receiving 550 complaints and challenges to public sector actors not complying with Estonia's freedom of information laws or the PDPA. The top priority of the DPI is facilitating inquiries into suspicious uses of personal information, and by helping constituents directly confront public sector actors through proper legal channels, the DPI is cultivating trust in public institutions and the e-services provided by them.

In a 2013, Eurobarometer study, the level of trust for governmental institutions in Estonia grew six percentage points to 44 percent, compared with an EU average of 27 percent. Trust in municipalities also grew to 60 percent in Estonia, compared with the EU average of 46 percent. From a United States perspective, a recent Pew survey showed 80% of Americans believe government surveillance should be a major cause for concern. The evidence speaks for itself when measuring Estonian's level of trust compared to other EU countries and the United States, but there is one other factor that has made the proliferation of e-government services successful in Estonia: Internet accessibility.

Reducing the "digital divide" by increasing access to the Internet and technological literacy should be a cornerstone for any nation wishing to expand e-governance capability. It would seem obvious to most: without Internet accessibility there can be no demand for e-governance. But, as seen in Estonia, working with the private sector to facilitate penetration in Internet markets can transform an unconnected society into an e-society. In 2001, 32 percent of Estonians consistently used the Internet. Today, that number has grown to 82.4 percent, with over 1,000 public WIFI hotspots currently, compared with 460 in August of 2002. With more inclusion comes more demand for the convenience of using e-services, and in Estonia, this has become ingrained in the culture of the information communication technology (ICT) community.

The catalyst for Estonian Internet connectivity is the emphasis of promoting public-private partnerships. One prime example is the 2010, "Come Along!" campaign, initiated for improving Internet literacy free of charge with training and informational sessions targeting 100,000 citizens (in both the Estonian and Russian language). Involving private Estonian telecommunication companies, banks, and public sector actors like the Look@World foundation, the concerted effort established 35 computer clubs throughout Estonia for educating citizens who may be disproportionately disengaged from using technology. Not only does this boost the economic prospects of citizens, it makes them more inclined to use e-services by enhancing familiarity with how the Internet works and mitigating the fears that come with using new technology. Programs like "Come Along!" can be an example in other countries that are willing to devote an adequate amount of resources to increasing internet accessibility and technology education in cooperation with the private sector.

It is remarkable how Estonia's technical infrastructure and e-services have flourished since regaining independence in 1991. Even more impressive is Estonia's recognition there has to be complementary legal frameworks protecting privacy in order to promote the usage of e-services. While no system can attain the abstraction of "perfection," Estonia at least has mechanisms in place where e-services are not viewed as a conduit for political leverage or illegal surveillance. As more countries provide e-services, the issue of online privacy will continue to be a leading question for constituents wary of technological advances connected to government institutions. While each nation has its own cultural and political context in decision-making, looking at the Estonian model of siding with citizens' right to privacy over state interest will only be beneficial for the growth and trust of e-governance.