Dankesworte

(Sprechzettel englisch)

von

Toomas Hendrik Ilves

Staatspräsident der Republik Estland a.D.

anlässlich des

Reinhard Mohn Preises 2017

Smart Country – Vernetzt.Intelligent.Digital.
Smart Country - Connected.Intelligent.Digital.

29. Juni 2017

Theater Gütersloh

Es gilt das gesprochene Wort.

Frau Mohn,
The board of the Bertelsmann Stiftung
Friends,

I am deeply honored to receive the Mohn Prize for 2017.

What Estonia has done in the past quarter century is the work of many people. I did outline what at the time was considered a quirky and impossible vision, but so many smart people took to the idea that soon Estonia was racing ahead on its own. It took a spark to light a torch that in turn was carried by many. Call it the Zeitgeist, one of the few German words English-speakers know.

At times, when good ideas ran up against silly, old-fashioned or ill-informed policy, I did my best unblock the path for those ideas to move forward and to prod those opposed to give it a chance. When bright ideas needed encouragement I always recalled how hard it was in 1995 to talk about digitization to a skeptical if not hostile public and, yes at times, an unconvinced government. This is hard to imagine today, when regardless of which parties are in office, e-Estonia has overwhelming public support. So thank you to all those courageous and creative people who have done so much to make Estonia what it is today.

After the past year or so, the digital world has become far more frightening than it was. We read daily of hacks, stolen data, invasions of privacy. We see our very own democratic systems under attack, in ways thought unconceivable or impossible a decade ago. The Bundestag, Emmanuel Macron's campaign and the Democratic National Committee servers are broken into, and private correspondence stolen. These are posted on line, at times in altered form, generating fake news. Robots or bots on social media rebroadcast these fake or falsified stories and hoaxes to millions of accounts and these are then rebroadcast. Social media itself allows Big Data analytics companies to profile and then target individuals in ways never done in the past. And finally (at least at the time of writing this), voting rolls are hacked, voters' data stolen by a foreign power. To what end? We don't know yet.

All of these disruptions I just listed make us worry. Some, the Luddites, want to stop and turn back the clock to a paper age. Others, for different reasons, instead want to increase "security" by restricting our freedoms and privacy. And then there are those who do not wish to take the steps needed to guarantee both our electoral democracy in the digital age or our security, all because of a lack of understanding.

Let me be clear: security in cyber does not and cannot come at the cost of freedoms. And Estonia is proof. Last week the UN's International Telegraph Union, nowadays better known as the ITU, the UN body responsible for Internet issues, published its survey of cyber-security around the world. Estonia ranks in first place in Europe, better than any other country, where number two, Norway is not even in the EU.

Internet security, however, has not come at the expense of freedom In its survey, Freedom House ranks Estonia as number one in the world in Internet Freedom. Internet freedom in Russia, on the other hand, ranks as "unfree" clocking in at 65th out of 88 countries surveyed.
Of course cyber-security can be obtained in a number of ways. Russia, for example, is number one in cyber-security in the CIS post-soviet space. All the more reason to look at other measures, such as Internet freedom in order to assess the interaction between security and freedom, something too often cast as a trade-off.

What these two studies, taken together, most clearly show, is that there is no necessary trade-off or contingent relation between security and freedom. You can have both. This is especially important to keep in mind amidst the barrage of proposals across the democratic West that in the internet era it is necessary to compromise on freedom in order to guarantee security. The UK government, US Attorney General Jeff Sessions and EU Justice Commissioner Věra Jourová all want to mandate “Backdoors”, encryption keys in the hands of governments (or the EU Commission). Related proposals abound.

Of course, this recourse to backdoors is a result of a spate of terrorist attacks in Europe and the US, where it is asserted that terrorists used encryption to thwart authorities listening in on their communications. Never mind the series of embarrassing revelations that authorities had been given advance warning about concrete, known terrorists (in the Brussels, Berlin and recent London attacks). Politicians still demand backdoors.

Rarely are such proposals reasoned. For one, even if backdoors are installed on one or another “app”, nothing prevents one from using a different encryption system. The only ones who would be subject to backdoors would be those who have no terrorist intent but value their privacy, which as we know is not guaranteed either in the case of telephony or SMS.

Secondly, as soon as a government, or even more preposterously, the European Commission adopts a backdoor, it becomes the Holy Grail of all hackers. What could be a more enticing either for prestige or financial gain than to steal the Keys to the Kingdom? Would we really entrust the European Commission or any national government for that matter to hold the keys to all encrypted communication? When even the CIA has been hacked with a series of zero-day exploits stolen, most recently allowing criminals to spread the WannaCry ransomware that inter alia brought down the UK’s National Health System

Nor do you need fear the skilled IT wiz-kid hackers who might break in. As NSA employees Edward Snowden and just recently Reality Winner have shown, “insider threats”, someone inside, who because of personal disgruntlement, ideology or money, can simply steal the keys, the holy grail. A recent collection by Matthew Bunn and Scott Sagan demonstrates that organization vastly underestimate the threat posed not by penetration from outside but from within. The effect, though, is the same as a hack: someone will obtain the keys to all encrypted communications, except for those who really want to use encryption and will use alternatives anyway.

What to conclude from this? For one, there is an appalling lack of thought about the implications of government mandated “backdoors”. It strikes me, as a former political leader, that my colleagues don’t really understand what they are proposing, the impossibility and the impracticality of such proposals.

To understand this issue, I have to go back to Estonia and a lesson I’ve learned over and over and shown empirically in last years World Bank Development Report, Digital Dividends, whose production I had the honor to co-chair.

The lesson is this. How we tackle this Brave New Digital World is an analog task. It comes down to policies, laws and regulations.

This is where a third study comes in. Yes Estonia has the greatest internet freedom in the world, and it has the best cyber security in Europe but a third study, this one by the European Union’s Digital Economy and Society Index 2017 rates Estonia as first in provision of on-line public services.
In other words, in this Hobbesian world of the internet, Estonians are both more secure and enjoy greater freedom, because we have taken care to offer our citizens security where it matters and let them be free where there is no need to force a fake security.
Let me briefly tell you what I think is needed.

1. You need a strong digital identity, guaranteed by the government, in Germany's case either the Länder or Berlin. Today, bad actors can enter your life not physically but on line. In the physical world governments demand and also issue passports in order to know who is who.

The digital world is the same. You need a strong digital identity.

2. To get the benefits of digitization, you need to give this digital identity legal status, i.e. to make a digital signature equivalent to a physical signature. All transactions requiring a physical signature must be possible with a digital signature. In Estonia there are only two transactions that must be done physically and in the presence of witnesses. Marriage and Divorce. But to do this, you must tie the digital identity to a national registry, just as you do with a passport. This is the link the German Bürgerkaart does not have and which is why you cannot do digital contracts.

3. The identity must be mandatory and universal. Why? If getting it is optional, optimally 15-20 percent of the population will take it. Look at it though from a private sector or even government point of view. Only 15 % of the population can possibly use a service, say digital prescriptions. Why bother spending the time and money to develop the service when 85% can't even use it? From a corporate or government policy perspective, though if you develop it, they will come. Estonia went in four months from single users of digital prescriptions to 98+ percent users. In four months. No one uses paper prescriptions, except for tourists.

4. Use the power of the ID to transform bureaucracy. Bureacracy is some 5000 years old. One thing has never changed. It has always been a serial process. A document, be in hieroglyphs on papyrus or on paper today – or even as attachment on an email will to one office, where it is approved, then to the next amt, to another, etc. One after the other. Serially. With a digital ID, all the necessary searches are done in parallel. This is why in Estonia we have a "once only" regulation, the government may

never ask you for information it already has. This is also why you can register a company in Estonia in 15 minutes and NB all of the same checks and controls used by other EU countries, where the serial, manual process often takes months.

5. Interactions with the ID must by highly secure. I won't go into it but we have encryption at RSA 2048, which I guarantee is not possible to crack right now. It must also be secure from the government. We know our system can work if and only if the citizen knows the government cannot look at his data- If the EU adopts a backdoor that includes Estonian citizens encrypted data, the our system will collapse. The citizen must be able to trust that his data are private.

6. You need the proper architecture of the back end. Indeed the back end, is the backbone of the system. We use a distributed data exchange layer, which means every interaction is direct between user and server, authenticated each time. It also means once you get into see what you are authorized to see, but you can't go beyond that. You cannot see other peoples data. Which means you can't steal other people's data.

All of these solutions are technological and digital but all these solutions require the analogue: policies, laws and regulations. That is the hard part, the technology is easy. Technology is everywhere and it is amazing cheap. Any government or state can get the technology. Moreover, our technology is actually old, meaning there is little we do that was not possible 25 years ago. Except that it wasn't implemented.

What then explains the huge difference between countries, even in Europe? It is the willingness of policy-makers to make policy, law-makers to enact laws and regulators, who have the backing of laws, to regulate.

Technology is digital, societies are analog. Unfortunately they have been for far too long considered disparate realms.

Let me give you two examples.

1. pre-snowden App. Tracking your travels via cell phone transmission lines
2. what is 2 to the 3rd?

This disconnect between science and democracy or between IT and policy has been what I have tried to bridge for the past quarter century.
Back in 1959 a British physical chemist at Cambridge, C.P. Snow, who was incidentally also a literary novelist, who coined the expression “the corridors of power” published an essay titled, “the two cultures” about these two worlds.

His metaphor: the dining tables at this Cambridge college.

He was the only one who could participate at either.

Today, what Snow described as a problem of the university is now a problem for all of us. Back then, TV-s didn’t look at us, phones didn’t listen in or follow our travels.

Today they do. Or can. These are policy, not technology issues.

Back then propaganda from foreign adversaries didn’t really reach the average citizen in Western Democracies.

Today through social media, they do. (Indeed just Facebook recently published a white paper admitting it had been manipulated in the 2016 election).
Indeed, today in elections not only in the US last year but also in ongoing and upcoming elections in Europe, digital means have been and continue to be used to manipulate the electoral process.

This most certainly is a policy issue. As fundamental a policy issue as can be in a democracy.

So I will end with this: a plea for policy-makers to learn what technology is about and for the geeks, those who devise the programs, algorithms and apps we use, to learn what a liberal democracy is. To understand that liberal democracies three pillars: free and fair elections, the rechtstaat or “rule of law” and fundamental rights and freedoms need to be preserved in this new digital age.