Presentation at Max van der Stoel Human Rights Award,
Jheronimus Academy of Data Science

Ladies and gentlemen,

What a wonderful place to pay our regards to the work of Mr Max van der Stoel and what a wonderful opportunity to talk to you about my grave concerns about the direction of technological development.

I studied history specializing in authoritarian regimes. That´s how, in the nineties, I first got acquainted with the work of Max van der Stoel. He mobilised the international community against the Greek Colonels regime (1967 - 1974), supporting dissidents and opposition politicians, visiting them at home in Greece while they were under house arrest.

In 1977, when Van der Stoel was Minister for Foreign Affairs he visited then Czechoslovakia and went to see an activist of Charta 77 and set a trend. From that moment onwards human rights behind the Iron Curtain came high upon the agenda of western European politicians. He made a difference.

If Max van der Stoel was still alive today, and active, would he be involved in human rights online? I hope he would. I think he would see how modern dictators use technology to spy on their citizens and use social media to influence their thoughts. Then again, he was an all-time friend of the US. So maybe we would not always see eye to eye.

But let me bring this back to here and now, away from foreign dictators to our daily lives online. To our right to privacy and data protection.

When my German green colleague Martin Häusling's assistant installed a browser plug-in called Web of Trust a while ago, she intended to protect her privacy better. Web of Trust would check the websites she was visiting against a community-maintained checklist and her visits to malicious websites were blocked. It made her feel comfortable and safer.

The popular plug-in was being used by a lot of privacy-minded people like her. She had no idea that every link she clicked afterwards was being recorded by the organization behind the plug-in and sold for data analysis. The data was anonymized, but still contained enough information to track her down. It revealed information about the political work of my colleague, including time and place of confidential meetings.

Her data was given away as a teaser by an Israeli company trading in data to a fake company, setup by reporters from the German TV-show Panorama. It was part of a 160 Giga Byte package containing the data of 3 million German users for the month of August of this year.

For my colleague, the revelation created huge problems, as it does for me. If I cannot trust to use the web, or let my advisors use the web, without every step being recorded, we cannot plan to talk to dissidents in foreign countries, we cannot meet with whistle blowers that have valuable information that we need to do our jobs.

Did we give away something important? Something fundamental, in order to create a free sample that generates business?

The amount of data we produce is growing exponentially. So is the accumulation of those data. What are the consequences? When that green dress you where shopping for online, continues to

hunt you down in the sidebars of your FaceBook wall, it is mainly annoying. When does an annoyance turn into a real concern? Is our data being used against us? Will it in the near future? Will the data crisis become an existential crisis for our democracy? It deeply concerns me.

Slowly we can see the focus of the big data industry is shifting from collection of our data to the creation of predictive models and algorithms through artificial intelligence. Decisions are becoming automated and ever less respectful to our fundamental rights.

Rachel Holmes, a former employee of Amazon, wrote in the Guardian, not a fortnight ago that technology is starting to control us.[1] I was deeply moved by her words and you will find that this speech is heavily indebted to her. We have become immune to the fact that our fundamental rights are being monetized. We are enabling the creation of an elite of companies that know it all and decide it all. That is something I am not comfortable with.

'Comfortable' is how we feel when we use Whatsapp to set a date for a girls night out. A friend with children tells me that in order to organise the weekend sports clubs and hobbies of their children, Whatsapp is THE tool. Not being on Facebook is rare. The online services we use - are designed in such a way that we are locked in. Comfortably locked in. My friends, who are very well educated and share with me a tendency to distrust big business, will dismiss any discussion of any alternative to WhatsApp, knowing fully well that it abuses their privacy, as I suspect you do too.

Not all of us have that luxury though. Sometimes someone's privacy abruptly disappears. You have probably heard about the gunman that showed up in a Washington D.C. pizza place to look for Hillary Clinton's child rape basement. This story is about fake news and how it spreads and pollutes the minds of people.

But it's also about the owner of the pizza place. His privacy was violently overturned. He was dragged into something that was vile and false and unjust. And it could have been worse if there had been more data about him and his pizza place available, that might have been used against him. And will he now forever be reminded of this trauma through every single Google search on his name? Forever half a suspect in the minds of people, of child rape and conspiracies? If privacy is intangible for most of us most of the time, we need to remind ourselves that it can become very concrete very sudden.

Another example
When one of my advisors, in the comfort of his home, installed an update to his home router, a pop-up showed up. Even though it was a router sold by ASUS, the pop-up requested him to allow the activation of a security product by Trend Micro. He did something you're not supposed to do: he read the license agreement.

That made him feel real uncomfortable.

The license allowed Trend Micro to monitor all traffic coming through the router, using Deep Packet Inspection, which means both the metadata and the content of the communication is being accessed. It also allowed Trend Micro to forward any data to its servers and to forward it again to its business partners for processing. This means that because he bought a router from ASUS he gave up not only his own privacy, but that of all other users of his internet access to a company that even included in the license the right to transmit the data to servers in countries that do not offer adequate protection.

1https://www.theguardian.com/commentisfree/2016/nov/28/technology-our-lives-control-us-internet-giants-data?CMP=share_btn_tw

This way, Trend Micro is ignoring the fundamental rights of its users and turning the self-bought internet equipment of ordinary people into surveillance machines. What actually happens to the data Trend Micro collects is impossible to tell. Maybe it only collects a very tiny and reasonable amount of data that really helps to secure your home internet and nothing else. On the other hand, they boast publicly that they receive 100 Tera Bytes of data every day – the equivalent of 7 pages of text for every person on earth every day. So that might be naive.

And the license agreement suggests otherwise as well. Did you know that Trend Micro is in an active partnership with Interpol, which involves Trend Micro handing over information based on this pool of data to Interpol, which itself lacks any clear oversight. Is my advisor paying ASUS to have Interpol watching his every online move? Is the fact that we cannot exclude that possibility not problematic in a democratic society?

That is only a single example. One that worries me, and that I am having investigated. But it is small beer. There are many more examples. How about the monitoring devices that are being installed in cars to lower insurance premiums and that can prevent the use of a smartphone and register when you're speeding? The Dutch Prosecutor's Office really wants these devices to be installed. Too close for comfort?

Already today, every new car produced for the European market has a SIM-card built in that will automatically call 911 if you have an accident. Safety first? How comfortable! Or maybe not when you know that the so called E-call chip contains a GPS chip that cannot be turned off.

And what about the predictive policing systems that are helping the police to allocate their resources, based on algorithms? When we know from research that algorithms tend to reproduce our existing biases and prejudices?

Did you get a present this week for one of your children or grandchildren? The Dutch celebration of Sinterklaas is only days ago. You might have bought them a nice doll. One that responds to what the child says to it. That is so cute and loved. Or is it a bit creepy as well? How would you feel if what your child says ends up on your Facebook wall in the shape of targeted ads? How would you feel if your child's play is being recorded and analyzed by automated systems for commercial and who knows what other purposes? Does that make you comfortable? This week toy stores in the Netherlands recalled a doll that was recording sound all the time and transmitting it to online servers in the USA that used speech recognition to influence the doll's behavior. But those data can also be used to spy on whatever goes on in the doll's home.

There are so many examples like these few that I've mentioned. And we do not know where the data goes to after it served its primary purpose. What if, say, one of the suppliers of Trend Micro or the doll manufacturer is a big company that has the capability to store a lot of data as well as the systems to more thoroughly analyze them?

Let's talk about Watson for a while. Have you met Watson? Most people know the system IBM designed as the winner of the US game show Jeopardy. That's the one we're talking about. There's something about Watson you should know.

Watson is a cognitive technology that approaches the way humans think and reason. Whatever that means, it can answer questions in normal language. It swallows huge amounts of data and then analyzes it to reach reasonable conclusions and it comes up with surprising results. Already it has correctly diagnosed people with hard to distinguish types of cancer. It is saving people's lives. Well done, Watson.

But that is not all it does, or IBM wouldn't be spending billions of dollars, buying company after company to get more data to feed Watson. What is Watson up to?

What if Watson is trying to unify the world's primary data streams? What precisely does it have access to? The little currents, like those of Web of Trust or Trend Micro, could very well end up on Watson at some point. In fact, Trend Micro and IBM have a long history of working together on security solutions.[2] It could easily swallow all sorts of anonymized data, since we do not legally protect the use of anonymous data. It's anonymous, so why protect it, right?

Well, it turns out Watson is really really smart. And it has access to a huge amount of anonymous data. And as we've seen in the case of Web of Trust, it is not always very difficult to re-identify data, especially if you have a lot of other data to compare it to. So maybe Watson is able do that. And if it is not, it still might learn to do it in a few more years.

This is a problem. This defeats the instruments we have to defend the privacy of European citizens. The new General Data Protection Regulation, that was created to defend our data, does not protect anonymous data. And it might well prohibit the re-identification of anonymous data, but how do we enforce that, if it happens outside of the EU and only on the internal servers of a huge corporation?

This is the corporate side of things, but it doesn't end there. The corporate and the public have merged, to a degree. Watson might not just be working with personal data in order to give its customers a better way to estimate insurance or credit risks, or to offer an improved sales or ad experience. IBM could also be working with the US National Security Agency. Even if they claim they don't.[3] They would have to, under US law, if ordered, and keep silent about it. Even if the Obama government is promising that it will not engage in mass surveillance of EU citizens, that says exactly nothing about the intentions of President Trump. I do not want to speculate any further. I will leave the consequences of such a system up to your imagination.

As a citizen I like to be safe in the society I live in, trusting the legislative authorities and feeling comfortable with the digital tools I use. I use them in a democracy, so they must be okay. As a politician I want to be able to provide such a trustworthy society to our citizens. But can I?

Last week, I proposed, as Rapporteur for the European Parliament, a series of new ways to prevent companies from using trusts, shell companies to evade their tax obligations. These new rules will help us get a better handle on international businesses, but it will not be enough. We need to also change the laws that enable the use of tax evasion schemes. We need to design laws that resist tax evasion. And the only way we can do this is if we do not allow the companies and people that benefit from tax evasion from writing the new rules. And we need more transparency about the way tax offices help businesses keep their taxes low.

The same is true for data. We see that companies like Trend Micro are effectively trying to evade the law. They find ways around the law to do whatever they want. Some companies might use anonymization, knowing they will be able to re-identify the data at some point or time or location.

I was there when the European Parliament negotiated the new data protection law. I felt the pressure by the corporate lobbyists advocating for a 'fine balance between privacy and commercial interests'. I saw how Commissioners like Neelie Kroes and Günther Oettinger protected the interests of the big tech firms. In the end we designed a law that will be a model for the way the world treats personal data. It is a strong law that demands changes in the way online services

---

2http://newsroom.trendmicro.com/press-release/channel-partner-news/trend-micro-experts-and-customers-share-cloud-security-insights-i

3http://www.zdnet.com/article/ibm-denies-assisting-nsa-in-customer-spying/

operate. Tracking without consent will become illegal and fines can be steep. But despite the great work done by my Green colleague Jan Philipp Albrecht, who was the Parliament's Rapporteur on the dossier, plenty of loopholes became part of the new law,that will enable dedicated companies to continue to use our data to develop their parasitic business models.

So can I provide you this high trust society where you can comfortably use your digital tools? They say that once you've seen a sausage being made, you never want to eat one again....
We need to move beyond corporate interests and reclaim politics as the home of the interests of its citizens and we need to close the loopholes that are part of the new data protection laws.

What is also politics, and economically sensible is something we can do:
We need to start making a much more serious effort to invest in the development of our domestic, European IT industry. We have neglected this. Why is there no European Google or Amazon or Facebook?

And, for that matter, where is that real European Cloud under real European jurisdiction that delivers improved privacy protections to European companies afraid of commercial espionage from outside the Union and to Member states that deal with sensitive data of their citizens. Such a European Cloud would also be highly attractive as a safe place for people and companies from countries without proper protection of the Rule of Law. KPN offers something like this, and although it's not bullet proof, at least it recognizes the competitive advantages.

Let us not copy-paste the American example of the monolithic tech firms, but adapt a European style. Wouldn't it be great to have a wealth of different tastes to choose from? Wouldn't that be much more comfortable, effective and creative, not to mention easier to keep in check? Not a single search engine or social network or cloud provider that can compete with US counterparts, but a lot of smaller, more efficient and creative solutions that compete with each other, but also work and create together. This can be done, but the Commission needs to rethink its strategies and change its advisors. Our core focus should be on creating the conditions that favor technological innovation by Small and Medium size Enterprises.

This will also improve the way we can deal with the privacy crisis. Smaller companies can adapt their business models faster when laws change. Even better: they have less impact on legislation, are more sensitive to the needs of their users and are more flexible in finding better solutions. And they are also more easily disciplined if they don't respect our rights.

That alone won't do it. Because we have to face the fact that the internet is a global phenomenon and that it will be necessary to ultimately solve these problems on a global scale, or at least have a better framework to deal with issues. Just as we will need new global mechanisms to deal with tax evasion, we will need new global mechanisms to deal with privacy evasion. Can we not design a system that centers on the interests of people everywhere? One that creates understandable, practical and enforceable rules that will hold true anywhere?

Such a system would create clarity about to whom personal data belongs and who can use it to create shareholder value. It would specify new limits on how states can use personal data to combat crime and terror, so that our citizens can exercise their freedoms in the full knowledge that no state, nor any corporation, will try to infringe on them unless it's urgently necessary and embedded in safeguards.

I propose drafting a global privacy and data protection treaty that protects the citizens of the world, in countries where privacy and fundamental rights often becomes a matter of life and death as much as in our lands of the supposedly free.

This is urgent. But you won't see that sense of urgency reflected in our current laws. And that makes me uncomfortable as a politician. So let's change the system from within. Let's, as citizens and as politicians, take our own responsibility and listen to the people that understand how the technology works, or that do read the license agreements. They will help us figure out ways to protect ourselves in a world that is not setup to protect us. If they tell us that using Whatsapp is a bad idea, then we should ask them what we can use. And if they tell us that a law, like the British Snooper Charter or the Dutch proposal on intelligence companies or police hacking are really bad ideas, we need to take that seriously and reject them.

We should be ashamed as Lawmakers that we need Austrian students to point out our failures to protect fundamental rights. Like Max Schrems did last year in the case he brought against Facebook and against the Commission's decision to OK the transfer of personal data to US companies. And we should be ashamed on behalf of the Commission that instead of using that urgent advice from the Court to change its ways, it could not apply a band-aid fast enough in the shape of the new Privacy Shield arrangement. The Commission is enabling big business' addiction to your data. How can me make them see how wrong they are?

Here I can pick up my role again as politician: a citizen goes to court and forces us to review the law. That's the comfort of a functioning Rule of Law upholding our fundamental rights.

And so it comes down to this: we are faced with a question that is fundamentally one of politics and of political power. Individuals are unable to prevent the collection and use of their data. Collective action is necessary. It is also easy. We simply need to change some rules, so they actually support our fundamental rights, not erode them. And then we need to continue to build our comfortable lives within those rules.

This is a fixable problem.

So let's start to implement the solutions that I have laid out for you today. Let's stop the madness of 'balancing' the fundamental rights of citizens with the interests of businesses. Let's demand a European action plan that boosts privacy friendly innovation in smart solutions through small and medium size enterprizes. And let's start writing a new international treaty that will safeguard everyone's privacy.

And above all we should hold strong to our commitment to our fundamental rights and build our laws and our world around them, just as Max van der Stoel always emphasized. We need them to support our liberty and, indeed, our comfort. In Donald Trump's brave new world, more than ever.