The Totalitarian Dystopia of the World Economic Forum is Becoming Reality

April 11, 2020 | In January 2018, a pilot project for the surveillance of air travelers, commissioned by the World Economic Forum, was agreed upon in Davos. At the time, I presented the Known Traveller Digital Identity (KTDI) project as a "totalitarian dystopa". A follow-up report shows that the multinational corporations are successfully involving governments and the EU in their plans. Covid-19 is speeding up implementation tremdendously and Bill Gates inadvertently lets us know how.

Like the 2018 report called „"The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel“ this more technical KTDI White Paper that goes by the title "Known Traveller Digital Identity Specifications Guidance" was published without any fanfare on the Internet in March. These reports, prepared by the consulting firm Accenture, are meant to be read only by people in the digital surveillance and security business. For understandable reasons, these people prefer to talk about digital identity rather than digital control or surveillance.

This is how the KTDI-scheme is supposed to work: We upload information about us into a database - or authorize others to do so. First of all, this should be a proof of identity from the authorities, but also our travel history, bank data, hotel accommodations, rental car bookings, documents from universities, government offices and much more. If we want to cross a border, we give the authorities access to this database in advance, so that they can see beforehand that we are harmless. Using facial recognition and our (ideally) biometrically linked smartphone, they can recognize us at the border crossing. If we have been diligent enough in providing data, we will be allowed to walk past the queues of other travellers, receiving preferential treatment and minimal checks. However, as it says in the first KTDI-report, if there should be any doubt as to a traveller's intentions, the border official can, on the basis of the information provided in advance, ask the respective person more in-depth questions, for example „to better understand his recent activities".

One can easily imagine how "voluntary" this data release will be once the system is established. It will, be of the sort: you can freely choose if you want to come into the country and hand over the key to your data, or if you prefer to stay out. A test-run is already being carried out by the border authorities of Canada and the Netherlands, with the airlines KLM and Air Canada at Amsterdam, Toronto and Montreal airports.

Participating corporations, such as Visa and Google, are not developing such a system for the police authorities at their own expense purely out of a cosmopolitan sense of duty. The 2018 KTDI-report, as well as the current White Paper, both state that self-monitoring at the border serves to create a critical mass of participants in the globally inter-operable data-sharing standard that is to be introduced.

The border authorities are simply the ideal catalyst for a global system of citizen-assisted mass surveillance and data sharing, gradually involving all the world's governments. Once the US and a few other large countries take part in that scheme, the citizens of a country whose government refuses to participate will have great difficulty travelling internationally.

Once all governments will have signed up to this standard for the forced voluntary exchange of data with citizens, it is envisioned that we will also be allowed to hand over our data in everyday interactions with companies and authorities. In both reports, health, education, banking, humanitarian aid and elections are the areas mentioned.

A global, totalitarian system

The KTDI White Paper makes clear the great ambition of the project in its conclusions:

> This paper outlines the ambition for KTDI to provide the foundations for a **globally accepted** decentralized **identity** ecosystem. Further development and wider adoption depend on maximizing **data exchange interoperability** and federated trust. Success will rest upon cooperation between world governments, regulators, the aviation industry, technology providers and other players to **establish global standards** and specifications for compliance by all stakeholders.

The conditions for enforcing this global surveillance standard are excellent. The Known Traveller project uses technical standards for verifiable credentials and decentralized identifiers as they are currently being developed by the World Wide Web Consortium (W3C) . W3C is the most important standards-setting body for the Internet and is dominated by US-American Internet and telecommunications companies.

W3C's members overlap strongly with those of the Decentralized Identity Foundation, which multinationals such as Microsoft and many smaller companies in the digital security industry have founded to advance global identity control standards. The companies that make up this group often have very close ties to the intelligence community. US Homeland Security has been involved in the Know Traveller project from the beginning. At the relevant digital identity forums, representatives of companies of the digital identity and security industries mingle with representatives of all the relevant security and intelligence agencies.

Forced voluntariness

The trick is the fiction of voluntariness, the explicit, if extorted, consent to the use of data, which you have to give every time you want to receive a government service in this system or if you just want to pay anything digitally. This is similar to what happens to you if you move around the World Wide Web today. You constantly have to voluntarily agree to monitoring requests of the website operators or simply choose to stay away.

The envisaged global system has a particularly pernicious aspect, which makes a mockery of the oft-advertized autonomy and control of those who supposedly own their data:

> Identity attributes are attested to and provided by issuing authorities (i.e. passport number, bank details. An issuing authority may also revoke a VC (virtual credential) that it had previously issued by updating the blockchain-based cryptographic accumulator accordingly..

Imagine what it will look like when this system is implemented as intended throughout the world, in every country, however repressive. Let us assume that the abolition of cash - which is being driven forward in parallel by more or less the same group of corporations and agencies - is successfully completed. For everything you want to do or pay, you depend on there being a tick in the right places in the database on you. If you fall out of favor with your own government, it might remove the tick from your identity information and screw you, even if you are not in the country. Your bank can do the same.

If this happens to you, you can try to keep it up for a while. But ultimately, you might have to do what the hero in the science fiction "Soleil à Credit" (Sun on Credit) by Michel Grimaud (1975) had to do. When his electronic card, which everyone needed to move around and to get rations, was confiscated by one of the automatic checking machines, he voluntarily reported at the prison gates and stayed voluntarily in prison until he was released, because otherwise he would have starved.

If the US government or the algorithms controlled by its agencies have someone in the world in their sights, they

can do the same thing. Either they get the respective government or banks to invalidate all digital documents of the target person, or the US internet corporations that control the system can do so, or the private US credit rating agencies slash the credit rating.

Much of this is already possible today and being done, though not frequently to individuals. But the system will only be comprehensive and perfect when there is a globally accepted technical standard that allows access to all these data and documents from anywhere. Only then will Washington (or rather Fort Meade and Langley) be able to control from their home computers everyone in every participating corner of the world. At the same time, national authoritarian governments will be able to control everyone in their own sphere of influence, whether they are at home or abroad.

This is the agenda behind the intense work that USAID, Gates and the World Economic Forum are doing, with the help of a dependent UN, to create digital identities for every person on the globe. They are working through ID4Africa, ID2020 and a dozen more such initiatives and consortia with ID in their names. (More on this soon in a follow-up post.)

Minority Report reloaded

Everybody can then be led by a normally unnoticeable nose-ring. It might get rudely pulled at, though, even if you didn't do anything at all, just because an algorithm concludes that you are a type that, statistically, might cause trouble soon, like in the movie "Minority Report". The ambition to get there is documented in the first KTDI report of the World Economic Forum with a highlighted quote from Google manager Rob Torres:

> Technology companies have made major strides in data mining, machine learning and artificial intelligence enabling enhanced **predictive analytics**. In combination with passenger-provided information, these technologies can be used by governments to … analyse complex patterns in big data with the goal of predicting border security risks.

The quote makes it clear that digital identity is not simply about giving everyone an easy way to prove who you are by means of a digital birth certificate or digital ID card, as they try to make us believe. If you are not yet convinced, here is another quote, taken from the "EU blockchain observatory report on digital identity and blockchain":

> When we say digital identity, we have to understand it as the sum of all the attributes that exist about us in the digital world, a constantly growing and evolving collection of data points.

Thus, digital identity means everything digitally storeable that there is to know about us, our actions and our preferences. It is about feeding everything known about a person into a database that can be tapped by all participating corporations and governments and manipulated by them at any time. Such that the corporations can steer us as consumer cattle into the right corral and fleece each of us individually and optimally, and have us as undemanding and obedient workhorses. It is about the governments and the corporations being able to detect anyone early on, who might want to break out of the system or break the system.

Remarkably, the World Economic Forum claims that it has not yet come up with a concept for the governance of this global totalitarian control infrastructure, i.e. who should be at the controls of this system. The White Paper says:

> Work on the definition and development of an appropriate governance framework for the KTDI concept

continues and will be addressed in a future report.

In other words, governments are supposed to commit themselves to this concept without it being clear who will pull the strings. In reality, of course, it is clear enough. It is Washington and the big US corporations, directly or through international bodies such as the World Economic Forum, W3C, FATF and many more, which they dominate. If you have any doubt about the ambition of the World Economic Forum to rule the world I suggest reading the following:

https://norberthaering.de/en/power-control/wef-un-2/

Governments and the UN have fallen in line

Nevertheless, governments and a UN dependent on corporate money seem quite eager to participate in this global surveillance system developed by multinational corporations and the US Homeland Security. It is marketed by participating companies in the security and identity industry under the euphemistic name Self-Sovereign Identity (SSI).

In Brussels, this term, SSI, is taking hold. The European Economic and Social Committee, an EU body in which employers' associations, trade unions and other interest groups are supposed to represent "organised civil society", has developed a European Self-Sovereign Identity Framework (eSSIF). It is almost one-to-one the dystopia described in the reports of the World Economic Forum.

The governments of 21 countries, including Germany, have formed a "European Blockchain Partnership" just three months after the World Economic Forum's 2018 meeting at which the Known Traveller concept was presented. This partnership seems to aim to advance the World Economic Forum's surveillance concept in its European incarnation eSSIF. One of the working objectives of this partnership, as stated in the Economic and Social Committee's presentation linked above, is to find out how to preserve European democratic values in the implementation of SSI. Good luck with that!

There are several more groups and partnerships at European level for the implementation of SSID and there are the various UN associated groups at global level. To take a closer look at them will have to wait for a follow-up blog post. It should have become clear already, though, that KTDI and SSI are not unrealistic ideals of Washington and the tech companies, but a realistic plan that is already being implemented on a global scale. We will not notice much of it until it is there.

Covid-19 speeds things up a lot

Governments' reactions to Covid-19 in South Korea and especially in Wuhan, China, and similiar schemes that are likely to soon be implemented in the West, are tremendously speeding up the global slide toward total algorithmic population control. In Wuhan, if you can't show a green button on your surveillance smartphone that signals that you are probably not infected, you are barred from most or all forms of public transportation and you are not allowed to enter restaurants or check into hotels.. In South Korea, recordings from surveillance cameras, credit card data and GPS data are evaluated to identify and track potential virus carriers.

In a video interview of March 24, the second richest and probably most powerful man in the world is interviewed by TED moderator Chris Anderson about the US corona strategy. In his usual relaxed power pose, Bill Gates talks as if he were President of the United States or head of the UN. The interview becomes particularly interesting when Gates comes to the presumed immunity of people who have already recovered from an infection. Gates links this to the issue of how and when travel restrictions can be eased by saying:

> Eventually we will have to have **a certificate** of who is a recoverd person, who is a vaccinated person, because you don't want to have people moving around the world where you have some countries, that won't have it under control, sadly. You don't want to completely block of the abilty of those people to go and come back and move around.

And then comes the doubly interesting sentence:

> So eventually there will be this sort of **digital immunity proof**, that will help facilitate the global re-opening up.

The latter sentence is doubly interesting because of the word "digital" and because the sentence is only contained in a slightly longer version of the video that someone has uploaded to preserve it. In the official TED video this one sentence was cut out (at minute 34:27) . According to the comments under the longer video, this happened in the afternoon of March 31st. This is astonishing, because the second half of the sentence about the reopening of the borders is actually a very good conclusion ot this topic, before the interviewer asks the next question. One would not cut it out for journalistic reasons. To cut it out for brevity, would not make much sense, because it is only two or three seconds long and the cut is noticeable.

It was presumably the word "digital" that was to be removed. For it invites questions that ultimately lead to all what makes up the Known Traveller program. In what is left in the official video, Gates speaks only of a certificate. This invites the following understanding of what he is talking about: Only those who have an immunity certificate from a health authority can book a flight, and only those who can produce it can board a plane and get through immigration. That would be quite easy to implement and relatively unproblematic.

Having the certificate in a digital version sounds more practical, because it would be faster and easier. But if a digital immunity proof for international travel is to be globally (machine-)usable, it needs a global standard for the certificate, a storage location for the certificates that is considered secure and generally accessible, a standard for data exchange that works everywhere, and a global standard for certifying the authenticity of a digital proof. The Known Traveller Program, which is being driven by the US Homeland Security and the World Economic Forum, wants to develop and implement all of this. Bill Gates is one of the most influential members of the World Economic Forum, if not the most influential.

Google and Apple come to the rescue

On April 10, Google and Apple have announced that they will cooperate in order to enable contact-tracking apps to be interoperable across the operating systems Adroid and iOS starting in May and to program the tracking ability into their own operating systems soon after. Contact tracing requires health authorities to be able to feed into the system, which telephone number is connected to a positively tested person. This can easily be supplemented by ticking the box for convalescence or vaccination.E voilá, the Known Traveller program is ready in a first application.

And as it should be, the voluntariness, the sovereignty over one's own data (Self-Sovereign Identity) is completely preserved. Everyone can decide for themselves whether they want to travel and use the tracking app, or whether they prefer to stay at home.

Since Google and Apple work closely and trustfully with the security authorities and secret services anyway, it will not be a problem to add further areas of application. First of all, the security authorities can check the box "may not travel" or "to be watched" if necessary. Even more interesting, the contact tracking feature can be used

to establish a network of contacts of people who are to be watched, and to add those contacts to the list. Beyond that, the system could be further refined as desired in the direction of what is outlined in the Known Traveller reports that Accenture has produced for the World Economic Forum.

Thanks to Covid-19, the Brave New World is taking shape much more quickly than anyone would have thought only three months ago. And thanks to Covid-19, many or even most people would currently find such totalitarian power desirable. Covid-19 is a heaven-sent gift for the World Economic Forum's plans.

German version (Part 1; Part 2)

To be continued soon ...

https://norberthaering.de/en/contact-and-free-newsletter/