Telescreen surveillance

Introduction

A lot of people are afraid that their government is observing them. Whether it is by bugging or by monitoring, they always find a way to express their fear by a conspiracy.

1984 reference

In Oceania, the citizens have very little to no true privacy. The goal of the government leads to total control over the population of Oceania. With different tools, the people get observed or bugged. The most common control instrument is the telescreen. In all homes and the work/public places telescreens with microphones are installed which watch and/or listen to people any time. In case of talking bad about the party, a voice shouts out and intervene. Those telescreens cannot be turned off if the owner is not a member of the inner party. Citizens are controlled, and the smallest sign of rebellion, even something as small as a suspicious facial expression, can result in immediate arrest and imprisonment.

Figure 1: Big Brother warning sign

This control measure leads to a dehumanizing life with no privacy. The residents are afraid to say or do something bad in the eyes of the party. So, they have no other option to follow the rule, accept the situation and do the best of it. Otherwise, as already mentioned, they will get punished and imprisoned. In the eyes of the government is it understandable to have such strict control measures. In this way, they can control everything that the population of their city is doing and what they are saying. But a goal of the government should be to provide an enjoyable habitant to live in and to have a happy and satisfied population. And this would not be a result out of it. But how is it nowadays?

In comparison to today, such measures would not be possible. One reason would be that people nowadays are too educated to be humiliated, and they would probably start a revolt. The telescreen from Orwell's 1984 violates human rights and cannot be part of modern society. But what are the telescreens of the 2000s?

Telescreen surveillance

Our actual situation in 2021

Recently, there has been voting regarding a law which is meant that every web user has the possibility to create an electronic identity to identify and authenticate her-/himself when surfing on the internet. In other words, it is the voting about the E-ID law in Switzerland.

Figure 3: E-ID rejection

The main idea of this new law is to help users simplifying the use of online services such as web purchasing and/or manage governmental stuff like passport renewals or official requests. It should help to get things done quicker and "safer". The citizens, however, have rejected this new law in the first run because they were afraid of a lack of data security which could have been occurred. The government wanted to source this business out to private companies which should have taken this task over for the government. The plan was that a particular company (unknown) which should have been chosen from the government, should have set up and manage all online ID registrations of citizens. The fear that data that would have been in the possession of a private enterprise instead of the government, which is considered more secured than an enterprise, resulted in a rejection of this legislative proposal. A retry, though, is in process. It is also important to mention that we actually have a similar form of the E-ID which was launched in 2010. It is called SwissID (formerly SuisseID). Its purpose is to use public services as mentioned above. Another point is also the actively listening phone microphone which leads also to personalized ads when talking about stuff in real life, for instance. It is confirmed that when we are talking about new shoes, for example, that after speaking the shoe brand out loud, a lot of shoes with the mentioned brand appear in Google ads when the web browser is opened and used. Actively listening and data evaluation are defined in the terms and conditions of apps or rather smartphones.

Figure 2: Logo SwissID

When we compare our actual situation of technology with the technological facilities mentioned in 1984, there are uncanny resemblances. We use computers or mobile devices with screens, and which are connected to the world wide web. The connections to these secured internet protocols are mostly officially regulated, so, that only the surface-web[1] with its allowed content automatically appears for web users. On one hand, this could be an advantage for web users, as criminals then would have few to no chances to act criminally on secured sites. On the other hand, data of citizens such as credit card details could be traced by enterprises due to logged web traffic. This is not even bad either, as credit card details are always strongly encrypted nowadays. But in the worst case of an anonymous cyberattack on their websites, confidential web traffic data

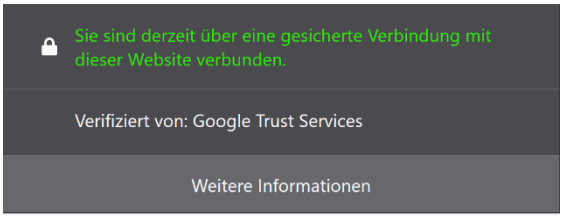

Figure 4: Secured connection notification

[1] *Part of the internet which is public for everyone (e.g., Google, Facebook, etc.)*

of people could be stolen and misused for criminal purposes, such as the Indian Banks data breach in 2016 where 3.2 million debit cards were compromised.

In 1984, the party also knows everything about its people but in its context is more described as something bad because they know everything about their citizens and punish disloyalty. In our actual situation, the strive for “omniscience” of the Swiss government regarding electronic identities is not something bad in the first place, as they try to reduce online criminality and fake identities and make web services easier and more convenient to use. But what will happen when these so-called “strives” go too far? What will happen when the government starts to decide which websites people can access in the future? Will they start to trace their citizen’s activities and intervene if someone defames them online?

Scenario 2084

A possible scenario in 2084 is that the E-ID concept has been around for a long time. All citizens must be registered for an electronic ID account when they want to use the internet. When people sign up and log into their accounts, they will be able to see a dashboard with all their stored personal data such as name, photo, ID/account number, date of birth, payment method (credit & debit card, cryptocurrency[2], etc.), vaccine certificate, diplomas, etc.

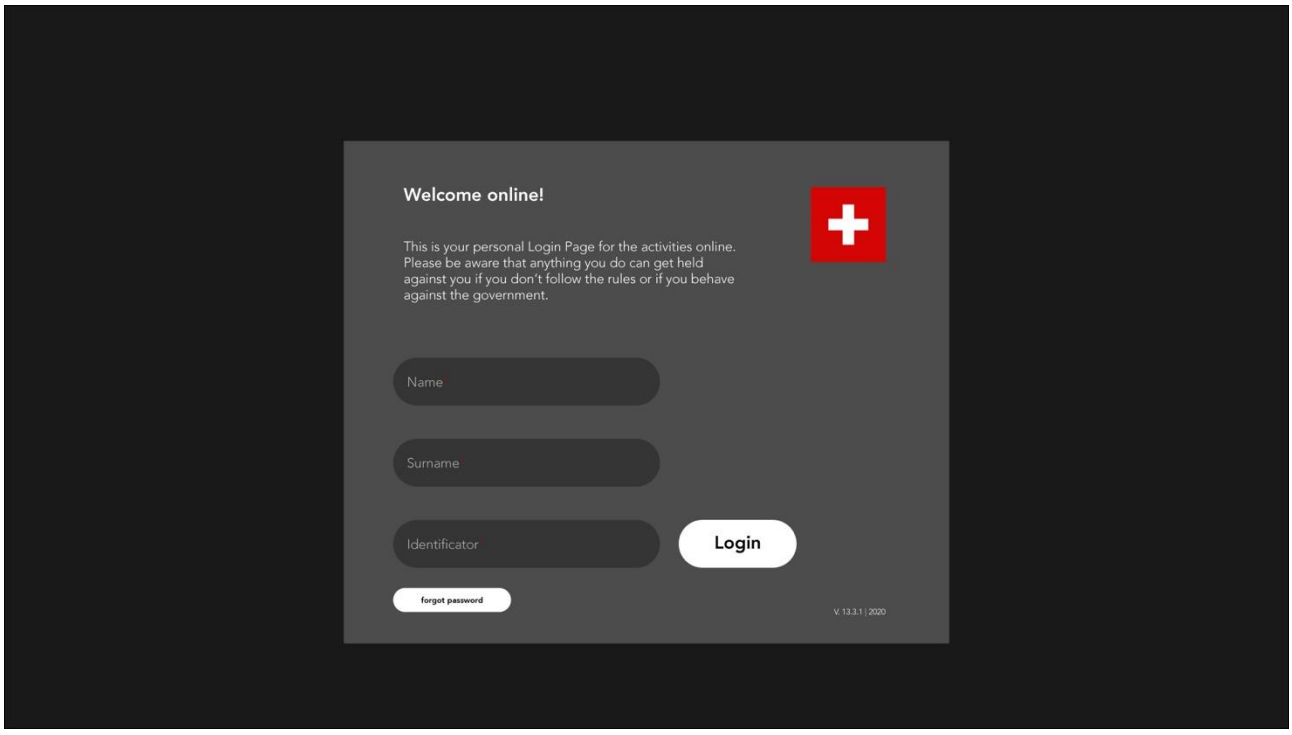

Figure 5: E-ID Login

Since all web traffic must go through this initial authentication process, whether with a computer or via mobile phone, the government will be able to see all data of every citizen. This will lead to some advantages and disadvantages. The advantages of such a system will be clean internet with no fake accounts or e-mail addresses which could scam gullible people.

[2] *Digital payment method beside US Dollar, Euro, etc. which is running on blockchains (e.g., Bitcoin, Ethereum, etc.)*

Telescreen surveillance

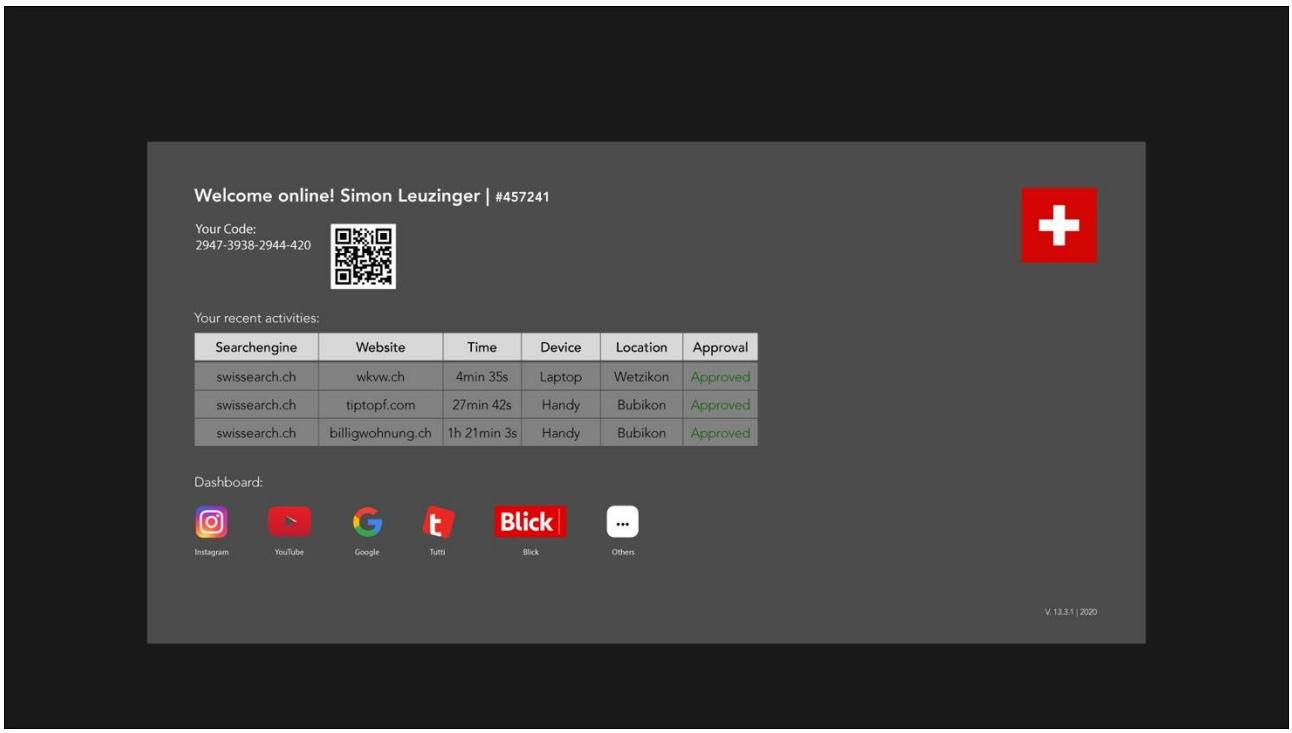

Figure 6: E-ID Dashboard

Another positive aspect is simplified inquiries when opening a bank account or request passport extensions. But this would also lead to some privacy violations, but which is, in this future scenario, inevitable as the creation of such an electronic account is governmentally mandated. People who do not want to use the electronic form will not be able to claim any governmental or corporation-specific services. They could be also fined for not having an electronic identity card, which could replace physical cards and make them invalid. Another negative aspect of these authentication measures will be the governmental control over people's money. For talking bad about the regime, the police would be able to locate the "troublemakers" as they are easier to identify on the web and they would freeze the assets of this person and withdraw the penalty fee for bad talking automatically. In the worst case, they could punish with imprisonment or restrict their internet access.

Conclusion

In conclusion, the E-ID law which, most likely, could come up again, could open new possibilities for the government to have a look at their citizen's personal data. This concept of cleaning up the data traffic could be developed more and more and could result in a situation in 2084 which is mentioned above. In the end, the government has all data needed to shut down a person's "existence" even if it is just online. They could be able to see all our interests while browsing, our purchases, our social media, our education level and the money in our accounts. Then, the sentence *"**Nothing was your own except the few cubic centimetres inside your skull.**" (p. 32, l. 1-2)* would become a reality to some extent.

Telescreen surveillance

Sources:

https://www.blick.ch/brand-studio/so-koennen-sie-sich-schuetzen-belauscht-mich-mein-handy-id15919724.html

https://www.e-id-referendum.ch/

https://en.wikipedia.org/wiki/List_of_data_breaches

https://www.dw.com/de/twitter-donald-trump-sperrung-usa/a-56177398

https://www.watson.ch/!893044714?utm_medium=social-user&utm_source=social_app