ID2020, Known-Traveller und Kontaktverfolgung durch Google und Apple: US-Konzerne werden zur Weltpassbehörde

16. 04. 2020 | **Hören** | **Wir sind nicht mehr weit davon entfernt, dass die digitalen Technologiekonzerne der USA virtuelle Passbehörde der Welt werden, die bestimmt, wer sich in welchem Radius bewegen darf. Sogar die physischen Kontakte jedes Trägers eines Android oder Apple-Smartphones sollen künftig erfasst und von den USA aus auswertbar sein.**

Beim Davoser Milliardärsstelldichein 2018 hat das Weltwirtschaftsforum in Zusammenarbeit mit der US Homeland Security das Pilotprojekt „The Known Traveller Digital Identity“ vorgestellt, mit dem letzlich alle international reisenden Weltbürger genötigt werden können, Daten über sich zu sammeln und diese bei Grenzübertritten „freiwillig“ herauszugeben. Wenn das einmal etabliert ist, solle es auf alle möglichen weiteren Anwendungsgebiete ausgedehnt werden.

Das Weltwirtschaftsforum lässt eine totalitäre Horrorvision wahr werden

19. 02. 2018 | Der Milliardärs- und Großkonzerneclub Weltwirtschaftsforum hat sich mit staatlichem Segen für die Verbesserung der Kontrolle von Reisenden zuständig erklärt. Dafür haben die Konzerne eine Serie von Workshops organisiert, an der die US-Homeland Security und andere staatliche Einrichtungen mitmachen durften, weil sie das Ergebnis ja später umsetzen sollen. Heraus kam eine Horrorvision … weiterlesen

Dieses Projekt ist Teil eines umfassenderen Überwachungsprojekts, das die Hauptakteure parallel dazu, und schon etwas länger, vorantreiben. Unter dem Namen ID2020 wollen die US-Konzerne, die die digitale Welt

heißt das im Titel des Aufsatzes einer leitenden Weltbank-Managerin. Identität ist dabei aber weit über ein übliches Ausweisdokument hinausgehend zu verstehen, als alles was es an Interessantem über eine Person, ihre Aktivitäten und ihre Vorlieben zu wissen gibt.

Wichtiger Bestandteil des Konzepts ist, dass die Nutzer sich grundsätzlich biometrisch, also mit Fingerabdruck, Gesichtserkennung oder Stimmerkennung bei ihrem Smartphone oder Computer anmelden, damit sie verlässlich ihrem Gerät und der damit ausgeführten Aktivität zugeordnet werden können.

Und nun kommt auch noch eine **Kooperation von Google und Apple** dazu, die unter dem Vorwand der Pandemie-Bekämpfung Mobiltelefone mit den beiden alles dominierenden Betriebssystemen Android und iOS mit der Fähigkeit ausstatten wollen, per Bluetooth-Technologie aufzuzeichnen, welche Personen sich in enger räumlicher Nähe zueinander befunden haben, und zwar über beide Betriebssysteme hinweg.

Dezentrale Speicherung und Nutzerautonomie zur Tarnung

Alle drei Projekte versuchen die politischen Entscheider und die Öffentlichkeit mit gut klingenden Orwell-Phrasen wie „Good Digital ID“, „self-sovereign identity“, oder „privacy-protecting, portable and user-centric digital identity“ (Privatsphäre-schützende, transportable und nutzerzentrierte Identität), oder Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) zu blenden, und ihnen vorzumachen, es ginge hier nicht um die Perfektionierung der Überwachung, sondern im Gegenteil um den Schutz der Privatsphäre.

Über die Horrorvision des Known-Traveller-Projekts habe ich schon zwei Mal geschrieben, einmal 2018 (siehe oben) und dann noch einmal vor Kurzem, als die US-Beratungsgesellschaft Accenture im Auftrag des Weltwirtschaftsforums, einen Bericht mit technischen Spezifikationen des Programms veröffentlichte. Accenture ist Nachfolgerin der im Enron-Skandal untergegangenen Anderson-Consulting, mit steuerbedingtem Sitz in Irland.

wird wahr gemacht

Hörbeitrag (extern) 8. 04. 2020 | Beim jährlichen Milliardärsstelldichein in Davos Anfang 2018 wurde ein im Auftrag des Weltwirtschaftsforums erstelltes Pilotprojekt für die Überwachung von Flugreisenden beschlossen, das ich damals als "totalitäre Horrorvison" vorstellte. Ein nun veröffentlichter Nachfolgebericht zeigt, dass der Club der größten multinationalen Konzerne eifrig und erfolgreich daran arbeitet, die Regierungen und die … weiterlesen

Das Weltwirtschaftsforum, die Lobby der weltgrößten multinationalen Konzerne, fühlt sich berufen und arbeitet eifrig daran, in Sachen Global Governance (Weltregierung) die UN zu überflügeln, beziehungsweise durch Instrumentalisierung der vom Geld der Konzerne zunehmend abhängigen Weltorganisation zu herrschen.

Widerstand gegen den Ausverkauf der UN an die Konzerne

25. 10. 2019 | Im Juni haben die Vereinten Nationen (UN) mit dem Weltwirtschaftsforum, dem Lobby-Club der größten multinationalen Konzerne, ein Abkommen zur Vertiefung der Zusammenarbeit geschlossen. Außer auf diesem Blog war das im deutschsprachigen Raum kaum irgendwo zu lesen. Nun haben sich über 200 internationale Initiativen, Organisationen und Gruppen zusammengetan, um mit einem offenen … weiterlesen

Wenden wir uns also ausführlicher ID2020 zu.

Berichte in den Massenmedien dazu findet man so gut wie nicht. Im Internet kursieren unter den wenigen kritischen Einlassungen vor allem reißerische

geschmeidigere Wege zum gleichen Ziel.

Allerdings haben Forscher in den USA **mit finanzieller Unterstützung der Gates-Stiftung** vor kurzem eine Art Bio-Chip namens Quantenpunkt-Tattoos entwickelt. Dabei wird mit zuckerbasierten, selbstauflösende Mikronadeln ein Impfstoff und gleichzeitg fluoreszierende „Quantenpunkte“ auf Kupferbasis injiziert, die in biokompatible Kapseln im Mikrometermaßstab eingebettet sind. Nachdem sich die Mikronadeln unter der Haut aufgelöst haben, hinterlassen sie die eingekapselten Quantenpunkte, deren Muster von speziell ausgerüsteten Smartphones gelesen werden können, um den verabreichten Impfstoff zu identifizieren. Die Forscher arbeiten daran, die codierbare Informationsmenge zu erhöhen (**Studie**). Noch wird dieses zwar praktische aber auch ziemlich gruselige Verfahren nicht angewendet.

ID2020 verfolgt einen anderen Weg. Auf dem ID2020-Gipfel 2017 bei den Vereinten Nationen haben Accenture und Microsoft einen ersten **Prototypen einer digitalen Ausweislösung** vorgestellt, die biometrische Identifikation mit einer dezentralen Speicherung von Identitätsdaten verknüpft. Dieser Prototyp basierte auf einer Blockchain-Lösung von Accenture und lief auf der Cloud-Plattform Azure von Microsoft.

Es handelte sich um eine Weiterentwicklung des Systems zur Erfassung der Identitäten von Flüchtlingen, das Accenture für den Hochkommissar der Vereinten Nationen für Flüchtlinge entwickelt hat. Damit wurden bereits Millionen Flüchtlinge biometrisch, also mit Merkmalen wie Fingerabdrücken und Iris-Scans, erfasst und gespeichert.

In den Entwicklungsländern setzt ID2020 vor allem darauf, im Rahmen von Impfprogrammen die Kinder biometrisch zu erfassen. Mit Neugeborenen hat man damit noch Schwierigkeiten, aber bei etwas älteren Kindern funktioniert das mit Fingerabdrücken und Iris-Scans schon gut.

Impfprogramme als Hebel

Im September 2019 hat ID2020 zusammen mit der von der Gates Stiftung maßgeblich finanzierten Impfallianz Gavi eine **Kooperation mit der Regierung von Bangladesch** verkündet. Im Rahmen dieser Kooperation soll „Impfung als Gelegenheit und Hebel genutzt werden, digitale Identitäten zu

Das System, das Microsoft und Accenture im Rahmen von ID2020 entwickeln, soll geeignet sein, nicht nur ein paar Millionen Flüchtlinge, sondern Milliarden Erdenbürger zu erfassen und den Zugriff auf deren Daten zu verwalten. Dabei sollen die Identitätsnachweise der Individuen diejenigen **ergänzen und auch ersetzen** können, die von den Regierungen der Heimatländer ausgestellt werden.

In der Blockchain sollen nur die Zugangsdaten zu den ID-Informationen gespeichert werden, die in anderen Datenbanken gespeichert sind, nicht die Daten selbst. Die Speicherung von Zugangsdaten in einer Blockchain soll sicherstellen, dass keine Regierung den Zugang auf Identitätsnachweise blockieren kann. Allerdings heißt es im 2020 veröffentlichten White Paper zum eng verwandten Known Traveller Projekt von Accenture, dass Aussteller von Identitätsnachweisen (Regierungen, Banken, Arbeitgeber, Vermieter) diese unabhängig vom Inhaber dieser Nachweise nachträglich für ungültig erklären können sollen.

Als Identitätsdaten gilt dabei alles, was jemand unter verifizierter Identität tut oder erleidet, also zum Beispiel auch alle Bankinformationen, Gesundheitsdaten und alles, was man über ein biometrisch mit dem Halter verknüpftes Smartphone tut.

Für das Jahr 2020 hat Accenture einen Prototypen angekündigt, der in der Breite getestet werden kann. Spätestens 2030 soll das neue System dann einen digitalen Identitätsnachweis für jeden Menschen bereitstellen.

Reales Machtgefälle wird angestrengt ignoriert

Was man von dem Autonomieversprechen halten darf, die Menschen könnten jedes Mal autonom entscheiden, ob und wem sie welche Daten für wie lange geben, macht das Known-Traveller-Projekt überdeutlich. Wenn man die Grenzer dazu bringen will, einen hineinzulassen, muss man eben alle Daten freigeben, die sie haben wollen. Dieses Machtgefälle gibt es regelmäßig, wenn ein Individuum etwas von einer Behörde oder auch einer größeren privatwirtschaftlichen Organisation will. Wer kann schon mit Amazon oder Paypal über die Geschäftsbedingungen verhandeln.

Daten propagiert haben, das Machtgefälle ignoriert und verschwiegen, das Datenautonomie durch vermeintlich freiwillige Freigabe zu einer Farce macht und in ihr Gegenteil verkehrt. Ich gehe hier von bewusster Täuschung aus. Das ahnt man schon bei dem grundlegenden Text **„The Path to Self-Sovereign Identity“** von Christopher Allen aus dem Jahr 2016, der als Erfinder des Begriffs Self-Sovereign Identity gilt. Allen preist die dezentrale Speicherung und Verknüpfung von Daten unter diesem Konzept als Beitrag zur Entmachtung von Microsoft an. In diesem Text erfährt man aber, dass er bald zu einem ID2020-Gipfel aufbrechen werde, um dort zu sprechen. Microsoft ist einer der Haupttreiber von ID2020, das sich die Self-Sovereign Identity mit Begeisterung zu eigen gemacht hat.

Nicht dass Allen das nicht hätte ahnen können. In seinem Text von 2016 beklagt er, dass all die ebenso gut klingenden Vorläuferprojekte zur Autonomiewahrung, aus denen sich Self-Soverign-Identity entwickelt hat, von mächtigen Institutionen gekapert und ins Gegenteil verkehrt worden seien.

Deutschland vorne mit dabei

Ein deutsches **Konsortium** unter Beteiligung der US-Unternehmensberatung Boston Consulting Group und einer Lufthansa-Tochter hat ganz im Sinne von ID2020 mit dem Aufbau eines digitalen Seuchenpasses begonnen, der genutzt werden soll, damit man Zutritt zu seinem Arbeitsplatz, einer Großveranstaltung oder dem Flugzeug bekommt. Die Informationen über Tests sollen über eine Blockchain zugänglich gemacht und über einen Identitätsprovider pseudonymisiert und DSGVO-konform in einer Cloud, also auf Servern von Amazon, Microsoft und Co. gespeichert werden. Nur der Inhaber des Zertifikats soll den Blockchain-Schlüssel auf dem Smartphone haben, mit dem man auf die Daten zugreifen kann.

Basis soll hier das vom Bundeswirtschaftsministerium geförderte **Lissi-Forschungsprojekt** sein, bei dem die Bundesdruckerei federführend ist. Lissi steht für “Let’s initiate self-sovereign identity”. Also genau die Phrasologie von Microsoft, Accenture und dem Weltwirtschaftsforum. Es wird auch wie bei ID2020 und KTDI mit den Open-Source Frameworks Hyperledger Aries und Hyperledger Indy gearbeitet.

konkreten Anwendungsfeldern umzusetzen.

Entmachtung der Regierungen

Für Menschen, die vor Nachstellungen ihrer Regierung geflohen sind, kann man noch gut nachvollziehen, dass Sie einen Identitätsnachweis bekommen sollen, der von ihrer Regierung unabhängig ist. Noch mehr kann man US-seitig diesen Wunsch verstehen, wenn es sich um eine Regierung wie die syrische handelt, mit der man einen unerklärten Krieg führt. Aber durch ID2020 soll es zur Norm werden, das Identität teilweise oder ganz von den nationalen Regierungen unabhängig wird. Dadurch werden die „Weltbürger“ teilweise von den Regierungen emanzipiert, außer von einer, der US-Regierung.

Von dieser Regierung, die den Standpunkt vertritt und auch durchsetzt, sie könne Gesetze erlassen, an die sich weltweit alle zu halten haben, werden sie maximal abhängig. Denn ihre Daten liegen dann in aller Regel auf Servern von US-Unternehmen, insbesondere den beiden führenden Cloud-Diensten von Amazon und Microsoft. Die technischen Standards wurden von diesen und anderen US-Unternehmen bestimmt, und die zentral verwalteten Zugänge zu diesen Identitätsdaten werden von diesen US-Unternehmen kontrolliert.

Maximale Sanktionsmacht für die US-Regierung

Nichts wird die US-Regierung davon abhalten können, Microsoft oder Amazon oder einem der US-Unternehmen, die die Blockchain-Architektur des Programms bestimmen, den Befehl zu geben, die Daten von Individuen oder Unternehmens auszulesen oder zu blockieren oder so zu manipulieren, dass die Betroffenen handlungsunfähig werden.

Selbst wenn sie es wollten, werden die Regierungen der Heimatländer den Betroffenen nicht helfen können. Sie stehen dann effektiv unter der hoheitlichen Gewalt der US-Regierung, ohne irgendwelche US-Bürgerrechte zu haben. Denn dass es die US-Regierung sein wird, die die Fäden in der Hand halten wird, darüber braucht man sich keine Illusionen zu machen.

Nächste Zugänge waren Mercy Corps, Hyperledger und das UN International Computing Center, sowie die Gates-finanzierte Impfallianz Gavi.

Durch das CLOUD-Gesetz haben die US-Sicherheitsbehörden Zugriff auf Daten auf allen Servern von US-Unternehmen, unabhängig davon, wo diese stehen.

Die 11 Mitglieder des **Führungsgremiums „Board“** und die Exekutivdirektorin kommen von oder hatten langjährige Beschäftigungsverhältnisse bei Gavi (zwei Mitglieder), Microsoft, Accenture, HP, Lehman Brothers, JP Morgan, UBS, OCC (Derivate-Clearing) und dem eng mit Google verbundenen Thinktank New America Foundation, ergänzt um eine kanadische Professorin und einen Haitianer mit UN-Hintergrund.

Aufteilung der Welt in Einflusssphären

China, Russland und ein paar andere Länder werden sich dem zwar widersetzen, sodass es zu einer Aufteilung der Hoheitsgewalt über die Weltbürger kommen wird. Europa jedoch macht fleißig mit, andere Industrieländer in der US-Einflusssphäre ebenfalls, und die von Finanzhilfen der Weltbank, des IWF und der Gates Stiftung abhängigen Entwicklungsländer sowieso.

Wenn das Bargeld einmal abgeschafft ist, wie es die in Washington ansässige Better Than Cash Allicance (US-Regierung, Gates Stiftung, Mastercard, Visa, Citi) ebenfalls unter Instrumentalisierung der UN betreibt ist die Überwachung und Kontrolle der Menschen und Unternehmen fast vollkommen, egal ob im Einflussbereich der USA oder in dem von China, das in dieser Hinsicht sogar schon weiter ist. Denn digitales Bezahlen ist eines der Hauptanwendungsgebiete der digitalen Identitäten und das Feld, über das deren Nutzung am effektivsten erzwungen werden kann.

Contact-Tracing durch Google und Apple

Vervollkommnet wird diese Überwachung und Kontrolle mit dem, was Apple und Google Mitte März angekündigt haben. Auf ihren konkurrierenden Betriebssystemen iOS und Android laufen weltweit fast alle Smartphones. Nun kooperieren sie, um zunächst ab Mai zu ermöglichen, dass sogenannte

Dabei wird auf den, aus Gewohnheit immer noch Telefon genannten Überwachungsgeräten dezentral gespeichert, in der Nähe welcher anderen Überwachungsgeräte man in den letzten zwei Wochen gewesen ist. Dabei ist jedes Gerät durch eine immer wieder wechselnde Nummer identifiziert. Wenn einer dieser Kontakte innerhalb der zwei gespeicherten Wochen als infiziert markiert wird, bekommen alle, die in seiner Nähe waren, einen Hinweis, der ihnen mitteilt, dass sie mit einem Infizierten Kontakt hatten und sich testen lassen sollten.

In den Folgemonaten wollen Google und Apple diese Funktionalität in die Betriebssysteme einprogrammieren, was die Performance verbessern und den Energieverbrauch senken soll. Die beiden Unternehmen betonen, wie sehr sie dabei auf Datenschutz und Dezentralität achteten. Viele Datenschützer sind auch halbwegs überzeugt. Aber: „Jedes dezentralisierte System kann man in ein zentralisiertes verwandeln“, **warnt Jaap-Henk Hoepman**, Professor für Privacy by Design an der Uni Nijmegen. Dafür braucht nur eine Stelle, deren App die Schnittstelle zu dieser Funktionalität nutzen darf, zum Beispiel die Polizei, oder ein Geheimdienst, diese so programmieren, dass bei Kontakt mit einer Zielperson nicht die Kontaktperson, sondern eine zentrale Stelle eine Nachricht bekommt.

Was ist absehbarer, als dass diese Funktionalität, wenn sie einmal da ist, für so etwas genutzt wird, wenn der nächste Kinderschänder zu fangen oder der nächste große Terroranschlag zu verhindern ist. Auch die Versprechen, die Maut-Daten nicht für Überwachung zu nutzen, hielten nur genau so lange, bis man die Möglichkeit hatte, auf diesem Wege publikumswirksam einen lastwagenfahrenden Sexualmörder zu überführen. Es war noch nie anders.

Quellen von Journalisten, die geheimes Material veröffentlicht haben, lassen sich auf diesem Wege aufspüren. Hat man Google-Home, kann Google alle Besucher dieses Hauses identifizieren. Gibt es eine Datensauerei, die Digitalkonzerne wie Google und Facebook entgegen allen Versprechungen noch nicht heimlich begangenen haben, weil sie dachten, es würde nicht auffliegen?

Großbritannien zu Datenschutzaspekten der dort geplanten Contact-Tracing-App beraten sollen..**Er hält** das Gerede von Datenschutz und Anonymität für Augenwischerei, weil das Contact-Tracing damit gar nicht funktionieren würde, unter anderem weil Trolle ein derartiges anonymes System sofort sabotieren könnten und würden, und sei es nur, dass klein Timmy sich als infiziert erklärt, um die halbe Schule in die Ferien zu schicken, oder dass ein Perforamencekünstler einem Hund das Telefon eines Infizierten umbindet und es dann durch den Park rennen lässt.

Contact-Tracing-Apps, die als erfolgreich gelten, sind ziemlich übergriffig in die Privatsphäre. Auswertungen, dass das automatische Contact-Tracing bei der Pandemie-Bekämpfung tatsächlich entscheidend hilft, gibt es nicht. Man muss sich ja vor Augen halten, dass das automatische Tracing sehr viel fehleranfälliger ist, als das manuelle, bei dem Infizierte nach ihren Kontakten gefragt und diese dann von echten Menschen kontaktiert werden.

Bluetooth geht auch durch die Wand, Viren nicht. Menschen, die längere Zeit in einer ordentlich Abstand haltenden Schlange vor oder hinter jemand Infiziertem standen, wird die App als möglicherweise infiziert warnen. Die Warnmeldungen würden wohl so zahlreich werden, dass die Menschen sie irgendwann einfach ignorieren. Alles was man sich ausdenken kann, um manuelle Korrekturen durch die Nutzer zu ermöglichen, geht auf Kosten von Datenschutz und Anonymität.

Auch zwei ausführliche Datenschutzfolgeabschätzungen zum vermeintlich Privatsphäre-bewahrenden Corona-Contact Tracing **vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung** (FifF) und **von Serge Vaudenay** von der École polytechnique fédérale de Lausanne, listen viele und schwerwiegende Möglichkeiten auf, wie die Anonymität von staatlicher Seite oder von Unternehmen aufgehoben werden kann, und wie die Betreiber und andere an die erfassten Daten kommen können.

> Wir müssen Bullshit beim Namen nennen, wenn wir ihn sehen und dürfen politische Entscheider nicht in der Illusion lassen, mit technischer Magie könnten sie den harten Entscheidungen entgehen.

Wenn etwa der Zugang zu Betrieben oder die Aufhebung von Bewegungseinschränkungen für einzelne davon abhängig gemacht wird, dass man sein Smartphone vorzeigt und damit nachweist, dass man die App regelmäßig nutzt, und sie keine Gefahr anzeigt, dann ist es mit Freiwilligkeit und Anonymität zu Ende.

Die Bluetooth-Protokolle der Anbieter sind außerdem notorisch für ihre vielen Sicherheitslücken, was sehr relevant wird, wenn alle genötigt werden, mit eingeschalteter Blootooth-Funktion herumzulaufen, oder das freiwillig tun.

Trotz all dieser bekannten und teilweise sehr offensichtlichen Funktionsmängel und Gefahren wird überall so getan, als wäre automatisches Contact-Tracing unbedingt notwendig, damit man einen Shutdown und Kontaktsperren allmählich aufheben kann. Das ist verdächtig, insbesondere weil es bei vielem Anderen, über dessen Wichtigkeit und Nützlichkeit Einigkeit herrscht, wie vermehrtes Testen und systematische Zufallstests zur Feststellung der Verbreitung von Covid-19, sehr viel zögerlicher vorangeht. Andersons Fazit lautet denn auch: „Wir müssen Bullshit beim Namen nennen, wenn wir ihn sehen und dürfen politische Entscheider nicht in der Illusion lassen, mit technischer Magie könnten sie den harten Entscheidungen entgehen."

Nachtrag (19. 04.): Jaap-Henk Hoepman hat einen langen **Folgebeitrag** zur GoogleApple-Plattform für das Contact-Tracing (GACT) geschrieben, der näher erläutert, wie damit eine (schlafende) aber jederzeit nutzbare weltweite Überwachungsinfrastruktur neuer Qualität geschaffen wird. Unter anderem schreibt er:

Unter einem anderen Blickwinkel betrachtet jedoch, schafft das einen enormen Hebel für die GACT-Plattform, weil diese damit praktisch zur einzigen Möglichkeit wird, Contact-Tracing per Smartphone zu betreiben. Mit diesem Schritt machen sich Apple und Google unverzichtbar. Sie stellen sicher, dass diese im wesentlichen globale Überwachungstechnologie uns aufgezwungen wird. Und als Folge werden sämtliche Mikrodaten in Zusammenhang mit einem Contact-Tracing-System auf Smartphones gespeichert, die sie kontrollieren. All das bedeutet, wir müssen Apple und Google in sehr hohem Maße vertrauen, dass sie die Nutzung der GACT-Schnittstelle durch andere sehr genau beaufsichtigen und dass sie GACT nicht selbst missbrauchen. Sie haben nicht unbedingt die makellose Historie, die solches Vertrauen rechtfertigen würde.

16. 04. 2020 • **Macht & Kontrolle** •

Corona, Digitale ID, UN, Weltwirtschaftsforum •

‹ Event 201 und die Bekämpfung von Fake News

Corona-Kapitalismus in den USA: hier zeigt er sich in Reinform ›