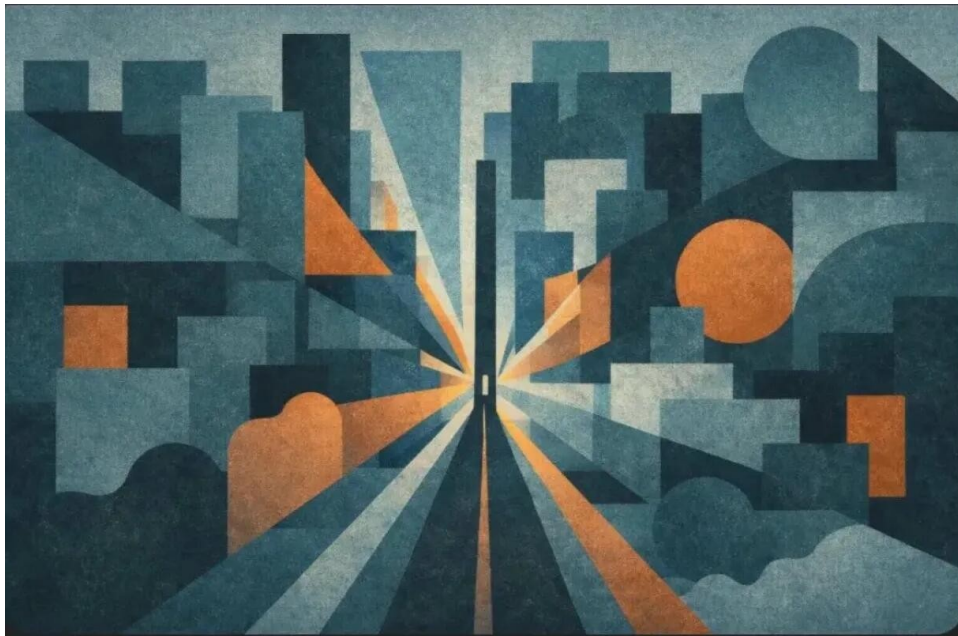


Warum die digitale ID eine Frage von entscheidender Bedeutung ist: Die Authentifizierungsebene



13. Juli 2026 | Joshua Stylman

Kürzlich hatte ich eine Auseinandersetzung mit einem Freund. Er ist klug, freiheitsliebend und versteht die Gefahr von digitalen Zentralbankwährungen (CBDC) nur zu gut. Geld mit begrenzter Gültigkeitsdauer, programmierbare Kontrolle, CO₂-Budgets – er erkennt die meisten Aspekte der zunehmenden Tyrannei ganz klar. Und doch tut er die digitale ID als Ablenkungsmanöver ab. Wenn ich versuche, ihm zu erklären, dass die digitale ID das Tor zum Gulag im Metaversum ist, verlangt er von mir, EINE Sache zu nennen, die eine digitale ID der Regierung ermöglicht, die sie bisher noch nicht tun kann.

Meine Antwort: Sie ermöglicht CBDC.

Natürlich haben Regierungen bereits in einer Weise in unsere Privatsphäre und Freiheiten eingegriffen, wie es sich unsere Vorfahren nicht hätten vorstellen können. Doch selbst angesichts des sich schleichend ausbreitenden Überwachungsstaates kann die Regierung eine programmierbare Währung nicht vollständig umsetzen, ohne dass bei jeder Transaktion eine authentifizierte Identität vorliegt. Sie sind Bestandteile desselben Ungeheuers. Die digitale ID ist die Authentifizierungsebene, während die CBDC die Währung ist, die darauf aufbaut.

Wer die digitale ID stoppt, verhindert, dass die CBDC in einem nennenswerten Umfang aufgebaut wird.

Die Institutionen, die dies vorantreiben – die üblichen Verdächtigen, darunter die Bank für Internationalen Zahlungsausgleich (BIZ) und die Vereinten Nationen –, äußern sich ganz offen über ihre

Absichten. In ihren eigenen Unterlagen wird es klar formuliert: Die digitale Identität ist eine Voraussetzung für eine zentralisierte digitale Währung. Und falls die Dokumente nicht klar genug sind, hätte Agustín Carstens, der ehemalige Generaldirektor der BIZ, ihre Ziele nicht deutlicher formulieren können:

Ein wesentlicher Unterschied bei der CBDC besteht darin, dass die Zentralbanken die uneingeschränkte Kontrolle über die Regeln und Vorschriften haben werden, die die Verwendung dieser Form der Zentralbankverbindlichkeit regeln, und dass wir zudem über die Technologie verfügen werden, um dies durchzusetzen.

Vielleicht sollten wir diesen Institutionen einfach Glauben schenken?

Wenn die Durchsetzung auf Autopilot läuft

Was mein Freund übersieht, hat nicht wirklich mit den Möglichkeiten zu tun. Es ging noch nie darum, was die Regierung tun kann. Es geht um die Kosten, die damit verbunden sind.

Derzeit erfordert die Kontrolle darüber, was man kauft, wohin man geht, was man liest – all das erfordert Einsatzkräfte vor Ort. Ermittlungen, Durchsuchungsbefehle, echte Menschen, die Entscheidungen treffen. Diese Reibung ist der Schutz.

Die digitale ID beseitigt diese Reibung vollständig. Was einst selektive Tyrannei war, wird zur universellen Tyrannei. Code schränkt Transaktionen je nach Konformitätsstatus ein. Eine menschliche Kontrolle ist nicht erforderlich.

Man kann sich das ganz einfach so vorstellen: Die Polizei kann gerade jetzt in deine Wohnung einbrechen. Die meisten Menschen machen sich darüber keine Sorgen. Würden sie genauso denken, wenn automatisierte Drohnen auf der Grundlage von KI-gesteuerten Kriterien gleichzeitig in jede Wohnung eindringen würden? Die Fähigkeit an sich ist nicht die Bedrohung ... sondern die Automatisierung in großem Maßstab.

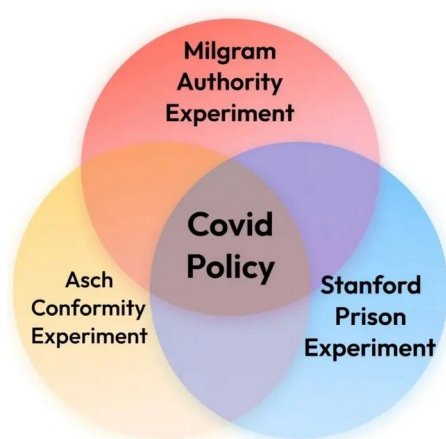
Und für alle, die jetzt denken: „Die Regierung hat doch ohnehin schon meine Sozialversicherungsnummer, und mein Handy verfolgt meinen Standort über GPS“ – ihr seht den Unterschied nicht. Derzeit sind diese Systeme voneinander isoliert – Ihre Bank weiß nicht, was Ihr Arzt gesagt hat, Ihre Kfz-Zulassungsstelle kennt Ihren Browserverlauf nicht usw. Die digitale ID ist die Interoperabilitätsschicht – ein Schlüssel, den jemand anderes kontrolliert – und widerrufen kann. Fünf Schlüssel für fünf Türen bedeuten, dass der Verlust eines Schlüssels verkraftbar ist. Ein Hauptschlüssel für alles bedeutet, dass jemand anderes entscheidet, ob Sie überhaupt Zugang erhalten.

Im Jahr 2021 brauchte man, um legal in meine eigene Kneipe zu kommen, einen Impfpass. New York City hatte zwar einen halbherzigen [digitalen Pass](#) eingeführt, aber damals war es größtenteils noch in Papierform. Dennoch war klar, wohin das führen würde. Als ich anfang, Freunde, Kollegen, den Typen im Café – eigentlich jeden, der mir zuhören wollte – zu warnen, dass dies ein Probelauf für eine digitale Identitätsinfrastruktur sei und dass der Kontrollpunkt, den sie gerade akzeptiert hatten, irgendwann programmierbar und dauerhaft werden würde, hielten mich die meisten für verrückt.

Nachdem ich lange E-Mails und nächtliche Tiraden satt hatte, begann ich, öffentlich zu [dokumentieren](#), was meiner Meinung nach auf uns zukommen würde. Es war schmerzlich offensichtlich, dass zentralisiertes digitales Geld Rationierungen, verfallende Ersparnisse und einen von Vorschriften bestimmten Zugang zum täglichen Leben bedeutete. Eine Art digitaler Käfig. Einige wenige Menschen in meinem Umfeld wurden hellhörig, doch die meisten spotteten weiterhin.

Ein paar Jahre später wird nun genau das eingeführt, was ich beschrieben habe – nur dass dieses System letztendlich nicht nur Impfungen betreffen wird, sondern jegliches akzeptable Verhalten definieren und regeln wird.

Wenn ich also höre, wie kluge Köpfe die digitale ID mit der Begründung abtun, dass „der Staat einen ohnehin schon überwachen kann“, macht mich das wahnsinnig. Du hängst an dem fest, was sie bereits tun können. Sie entwickeln etwas völlig Neues. Das ist so, als würde man zusehen, wie an jeder Straßenecke Blitzer installiert werden, und sagen: „Na ja, die könnten mir ja schon jetzt einen Strafzettel ausstellen.“ Sicher, eine Entscheidung nach der anderen. Stell dir nun vor, dass an keiner Straßenecke jemals ein Mensch beteiligt wäre. Die Grenzkosten sinken auf null, und die Entscheidung wird nicht von einer Person, sondern von einer Codezeile getroffen.



Das ist eine völlig andere Kategorie von Macht. Und nach dem, was wir alle im Jahr 2021 durchlebt haben – als wir miterlebten, wie unsere Nachbarn einen digitalen Pass als Preis für die Teilhabe akzeptierten, ohne mit der Wimper zu zucken –, haben wir gesehen, dass die Fähigkeit zur Gefügigkeit bereits trainiert ist. Covid war das [Milgram-Experiment](#), das [Stanford-Gefängnis-Experiment](#) und der [Asch-Konformitätstest](#) in einem, und unsere Spezies hat bei allen dreien versagt. Das Einzige, was damals noch fehlte, war die Infrastruktur auf gesellschaftlicher Ebene.

Die Titelgeschichte mag sich ändern. Die Agenda bleibt dieselbe.

Die meisten Amerikaner gehen davon aus, dass sie von solchen Dingen verschont bleiben. Vor einigen Jahren hatte die Mehrheit der Menschen, die ich kannte, keine Ahnung davon, dass überall auf der Welt massive Proteste stattfanden. Das lag zum Teil daran, dass sich unsere Medien nicht die Mühe machten, darüber zu berichten, aber auch daran, dass wir so abgeschottet sind. Und vielleicht ist das sogar beabsichtigt – denn Amerika wurde in einer Weise auf individueller Freiheit aufgebaut, wie es die meisten anderen Länder nicht waren, und genau dieser kulturelle Widerstand ist der Grund, warum sie die Infrastruktur zuerst überall anderswo normalisieren und sie dann als „internationale Best Practice“ hierher importieren. Und wir werden wie Schlafwandler direkt hineinlaufen.

Machen Sie sich nichts vor: Wenn Amerika diese Authentifizierungsebene akzeptiert, verliert der Rest der Welt seine letzte Möglichkeit, sich dagegen zu wehren.

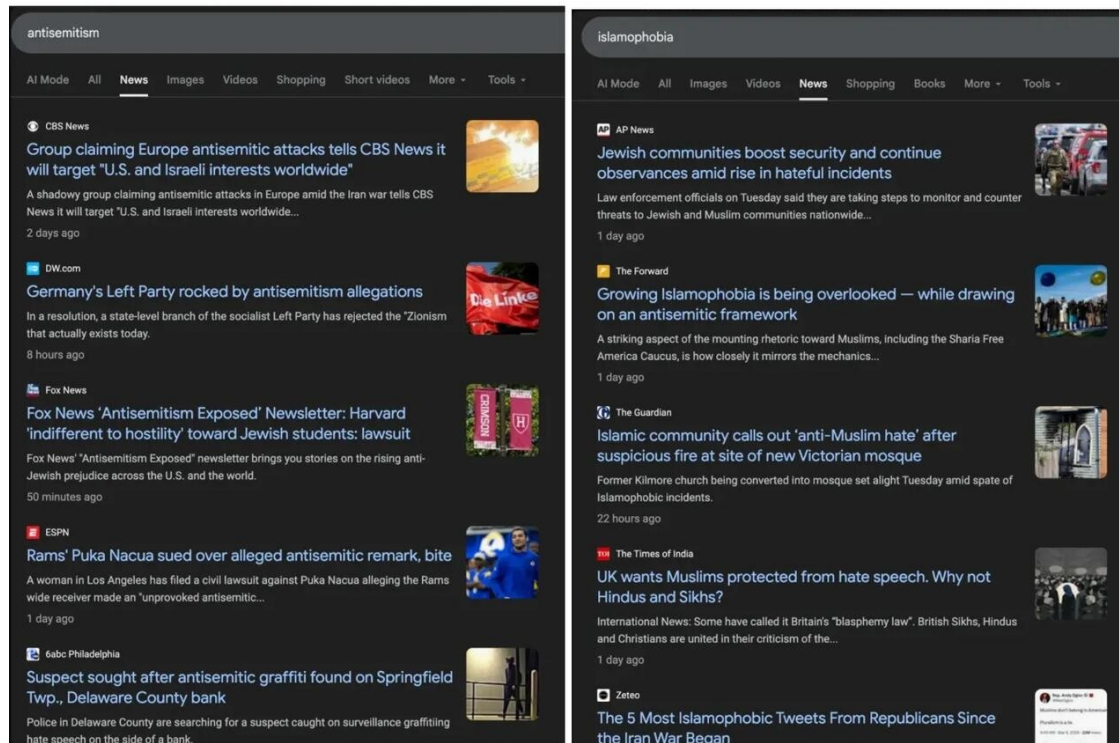
Ich möchte nicht auf einer toten Sache herumreiten, aber wir haben während der Corona-Pandemie einen Probelauf miterlebt.

Deshalb ist es keine Paranoia, darauf zu achten, was im Ausland geschieht – es könnte uns einen Hinweis darauf geben, was auf uns zukommt.

Das britische [Gesetz zur Online-Sicherheit von 2023](#) schreibt für Social-Media-Plattformen eine Altersüberprüfung vor, die mithilfe von „Ausweiskontrollen, KI oder Technologien zur Altersüberprüfung“ erfolgt. Premierminister Keir Starmer treibt die Umsetzung zügig voran – er nimmt Bestimmungen in das Gesetz zum Wohlergehen von Kindern auf, um „ein Verbot schnell durchzusetzen“. Durchgesickerte Protokolle von Sitzungen des Kabinettsbüros enthüllten, dass Minister über eine digitale ID für jedes Baby bei der Geburtsanzeige diskutierten. Eine parlamentarische Petition gegen die obligatorische digitale ID sammelte fast 3 Millionen Unterschriften. Dennoch wird das System eingeführt. Erst vor wenigen Tagen führte Apple die [Altersüberprüfung für alle Nutzer](#) im Vereinigten Königreich ein – Ausweisscans oder Kreditkartenprüfungen, um auf bestimmte Funktionen zugreifen zu können.

Die Briten versuchten, dies mit VPNs zu umgehen: Die Nutzung hat sich laut einem [Bericht](#) der Regierung mehr als [verdoppelt](#) – von 650.000 Nutzern pro Tag auf über 1,4 Millionen. Die Reaktion der Regierung? Sie stieß Diskussionen über [Einschränkungen für VPNs](#) an. Die Schraube dreht sich nur in eine Richtung. Identitätsprüfung vorschreiben. Wenn die Menschen diese umgehen, werden die Umgehungswerkzeuge eingeschränkt. Jede „Lösung“ erfordert mehr Kontrolle.

Einer meiner besten Freunde, ein Polizeisergeant, der nach 24 Jahren Dienst – ohne einen einzigen Tag zu versäumen – seinen Job verlor, weil er Impfvorschriften nicht befolgte, sagte mir, dass immer dann, wenn uns erzählt wird, etwas werde zu unserer Sicherheit getan, die Alarmglocken läuten sollten. Er hatte recht. Erinnert ihr euch an „Niemand ist sicher, bis alle sicher sind“?



Die Vorwand ist immer der Schutz. Schützt die Kinder, schützt Frauen vor Frauenfeindlichkeit im Internet. In letzter Zeit dreht sich alles darum, uns vor Antisemitismus und vor Islamfeindlichkeit zu

schützen. Blättert man an einem beliebigen Tag durch die Nachrichten, werden beide Themen im gleichen Rhythmus hochgespielt.

Es sollte selbstverständlich sein – ich habe keineswegs die Absicht, die echten Gefühle anderer herabzuwürdigen. Erst letzte Woche habe ich in „[The Enemy Is Not Each Other](#)“ ausführlich darüber geschrieben. Die Angst ist real, und die Menschen, die sie empfinden, haben Recht damit, sie zu empfinden. Mein Argument ist, dass die Infrastruktur, die aufgebaut wird, um diesen Gefühlen Rechnung zu tragen, der Käfig ist. Jeder emotionale Auslöser – ob echt oder nicht – wird zur Rechtfertigung für eine weitere Identitätskontrolle.

Australien hat ein eigenes Gesetz zur [Altersüberprüfung](#) verabschiedet. Kinder [umgehen](#) es bereits mit falschen Geburtsdaten und unregulierten Apps. Natürlich wird dieses Gesetz Kinder nicht in nennenswerter Weise schützen, aber es schafft auf jeden Fall eine neue Kontrollinstanz.

In Afrika werden von der Gates-Stiftung finanzierte [biometrische Ausweissysteme](#) unter dem Deckmantel der finanziellen Inklusion eingeführt. Die Vorwand variiert je nach Region – in diesem Fall „Hilfe“ versus „Schutz“. TikTok verlangt in Europa einen amtlichen Ausweis. [Discord](#) verlangt weltweit eine Altersschätzung anhand des Gesichts. Wie Fenigson es [formulierte](#): „Es ist genau dasselbe. Der einzige Unterschied besteht darin, dass man im Westen einfach mehr Ausreden vorbringen muss, damit die Leute es leichter schlucken können.“

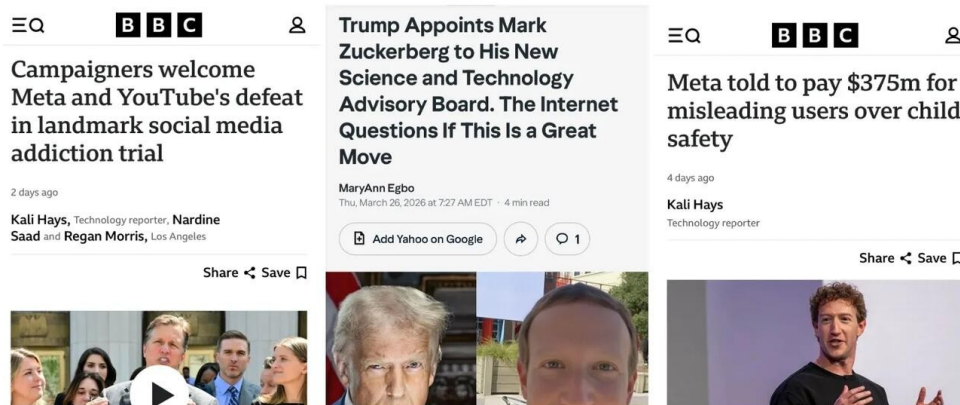
Und Amerika?

Kalifornien hat den Gesetzentwurf [AB 1043](#) unterzeichnet – ab dem 1. Januar 2027 muss jeder Anbieter von Betriebssystemen im Bundesstaat eine Altersüberprüfung einführen. Kein Gesetzentwurf mehr. Ein unterzeichnetes Gesetz. Eine Identitätsüberprüfung auf Betriebssystemebene, die in jedes Gerät integriert ist.

Und genau das hat Mark Zuckerberg unter Eid während seiner Anhörung vor dem Kongress zum Thema Kindersicherheit [vorgeschlagen](#). Seine „Lösung“ war verblüffend: Apple und Google sollen die Identität jedes Smartphone-Nutzers auf Betriebssystemebene für jede App überprüfen. „Es auf der Ebene des Smartphones zu tun, ist einfach viel sauberer“, sagte er. Im Klartext: Er wälzt die rechtliche Haftung von Meta ab, während zwei Unternehmen, die bereits unter kartellrechtlicher Aufsicht stehen, zu Identitätswächtern für das gesamte Internet ernannt werden.

Der Kongress verfasst die Gesetze, während die CEOs der Tech-Unternehmen das System entwerfen. Bemerkenswert: Erst letzte Woche befand eine Jury Meta – und YouTube – in einem [wegweisenden Rechtsstreit](#) der Fahrlässigkeit wegen der Schädigung von Kindern für schuldig, und in einem separaten Fall wurde Meta zur Zahlung von 375 Millionen Dollar verurteilt, weil es Nutzer in Bezug auf die Kindersicherheit in die Irre geführt hatte.

Das Unternehmen, das also gerade zwei massive Rechtsstreitigkeiten wegen der Schädigung von Kindern verloren hat, berät nun den Kongress dabei, wie die Identitätsinfrastruktur für das gesamte Internet aufgebaut werden soll. Was könnte da schon schiefgehen?



Ein parteiübergreifender Gesetzentwurf mit dem Titel „[Kids on Social Media Act](#)“ durchläuft derzeit den Kongress. Florida hat einen Gesetzentwurf zur Rechenschaftspflicht im App Store eingebracht, der Apple und Google dazu verpflichten würde, das Alter aller Nutzer zu überprüfen und personenbezogene Daten zu erfassen.

Wie Derrick Broze [hervorhob](#), steht im im März 2026 veröffentlichten „[National Policy Framework for AI](#)“ des Weißen Hauses der „Schutz von Kindern“ an erster Stelle, und der Kongress wird darin aufgefordert, Anforderungen zur Altersüberprüfung für KI-Plattformen festzulegen. Die Formulierungen sind zurückhaltend. Die Infrastruktur, die dadurch ermöglicht wird, ist dieselbe. Dies ist kein parteipolitisches Projekt. Beide „Seiten“ bauen es auf.

Und im März 2026 unterzeichneten mehr als 400 Informatiker aus aller Welt einen offenen Brief, in dem sie davor warnten, dass Vorschriften zur Altersüberprüfung Zensur, Machtkonzentration und den Verlust der Privatsphäre begünstigen – und dass die Systeme mehr Schaden als Nutzen anrichten könnten. Sie beschreiben damit die Authentifizierungsebene. Sie nennen sie nur nicht so.

Und im März 2026 unterzeichneten mehr als 400 Informatiker aus aller Welt einen [offenen Brief](#), in dem sie davor warnten, dass Vorschriften zur Altersüberprüfung Zensur, zentralisierte Macht und den Verlust der Privatsphäre begünstigen – und dass die Systeme [mehr Schaden als Nutzen anrichten](#) könnten. Sie beschreiben damit die Authentifizierungsebene. Sie nennen sie nur nicht so.

Es sind nicht nur Regierungen

Eigentlich braucht man keine staatlichen Vorschriften, wenn Unternehmen die Erfassung biometrischer Daten von sich aus zur Normalität machen. Und zunehmend muss man sich gar nicht mehr entscheiden – die Vorschriften verschmelzen mit Initiativen der „Big Tech“- und „Big Banking“-Konzerne, die alle auf derselben Infrastruktur basieren.

Ich habe diesen Punkt gegenüber Freunden angesprochen, die darauf bestanden haben, dass eine staatliche Digitalwährung (CBDC) vom Tisch sei, sobald der Präsident erklärt hatte, er werde sie [nicht einführen](#). Sicher, die US-Regierung mag das vielleicht nicht tun – aber was ist mit JPMorgan Chase? Durch öffentlich-private Partnerschaften können private Institutionen dazu gebracht werden, genau die Infrastruktur aufzubauen, von der die Regierung gerade versprochen hat, sie nicht anzurühren. [Wie heißt das noch mal?](#)

Im November 2025 führte [Apple](#) die „Digital ID“ in Apple Wallet ein, die es Nutzern ermöglicht, ihren Reisepass einzuscannen, Selfies aufzunehmen und zur Verifizierung „Gesichts- und Kopfbe-

wegungen“ auszuführen – woraufhin ihre Identität direkt auf ihrem Smartphone gespeichert wird. Die Digital ID wird von der TSA an über 250 Flughäfen akzeptiert und kann in 12 Bundesstaaten als Führerschein verwendet werden – Tendenz steigend. In der Pressemitteilung von Apple werden „weitere Anwendungsfälle für die Digital ID in der Zukunft“ versprochen. Der Anwendungsbereich ist von Grund auf unbegrenzt.

Vor kurzem [kündigte Discord an](#), dass die „Teen-by-Default-Einstellungen“ weltweit für seine 200 Millionen Nutzer eingeführt werden. Um auf altersbeschränkte Inhalte zugreifen oder die Sicherheitseinstellungen ändern zu können, müssen Nutzer eine „Altersüberprüfung“ absolvieren – natürlich mittels Gesichtsalter-Schätzung oder Vorlage eines amtlichen Ausweises. Discord führte dies zunächst in Großbritannien und Australien ein, [verzögerte](#) die weltweite Einführung jedoch nach heftigen Reaktionen – nicht, weil das Unternehmen seinen Plan überdacht hätte, sondern weil die Nutzer sich gegen die Umsetzung wehrten. Die Einführung steht weiterhin an, auch wenn sich der Zeitplan verschoben hat.

Die Argumentation ist immer dieselbe:

Apple: „Sicherheit und Datenschutz.“ Discord: „Sicherheit für Jugendliche.“ Zuckerberg: „Schutz von Kindern.“

Ich habe miterlebt, wie sich das in meinem eigenen Leben abgespielt hat. Freunde, die im Jahr 2020 noch über die Idee eines sozialen Bonitätsscores gelacht haben, zahlen heute für Clear und TSA PreCheck – und geben freiwillig biometrische Daten preis, um das Privileg zu genießen, die Warteschlange zu umgehen. Ich kann mich nicht daran erinnern, dass es jemals eine öffentliche Diskussion über die ethischen Auswirkungen davon gegeben hätte. Es ist einfach zur Normalität geworden. Das ist der „Compliance-Muskel“, der seine Arbeit verrichtet – die Fügsamkeit.

Und hier kommt der Clou: Die Datenbanken bleiben nicht getrennt. Sie werden verkauft, zusammengeführt, per Gerichtsbeschluss offengelegt oder gehackt. Bei Discords Altersüberprüfungssystem sind bereits bei einem einzigen Datenleck 70.000 amtliche Ausweisdaten [durchgesickert](#). Anders als bei einem Passwort kann man sein Gesicht nicht zurücksetzen. Sobald die Infrastruktur einmal existiert, stellt sich nicht die Frage, „ob“ sie mit staatlichen Systemen verbunden wird – sondern nur „wann“.

Ich würde behaupten, dass es hier möglicherweise ein zweites Motiv gibt, das während Zuckerbergs Anhörung niemand im Kongress näher untersucht hat. Als jemand, der sich seit 30 Jahren mit Online-Werbung beschäftigt, finde ich diesen Aspekt faszinierend: In einem Schritt, der den Nutzern ausnahmsweise einmal wirklich geholfen hat, hat Apple das [Tracking durch Drittanbieter](#) blockiert und den Nutzern die Möglichkeit gegeben, sich gegen die Nachverfolgung über verschiedene Apps hinweg zu entscheiden – was die meisten auch getan haben. Seitdem agieren Werbetreibende im Dunkeln und stützen sich auf fundierte Vermutungen darüber, wer Sie sind. Denken Sie daran: Zuckerbergs Vorschlag verlagert die Identitätsprüfung wieder genau auf diese Betriebssystemebene.

Eine Identitätsprüfung auf Betriebssystemebene löst das Problem der Werbebranche über Nacht. Ihre echte Identität, die auf Geräteebene bestätigt wird, ist mit allem verknüpft, was Sie auf dem Gerät tun. Das bedeutet, dass jeder Datenbroker, jeder Werbetreibende und jede Plattform, die derzeit mit probabilistischem Identitätsabgleich arbeitet, einen verifizierten Identitätsgraphen erhält – dank des Bundesgesetzes. Wunderbar.

Zuck schlägt kaum eine Lösung für den Überwachungskapitalismus vor ... er schlägt vielmehr dessen nächste Infrastruktur-Aufrüstung vor. Der Clou daran ist, dass er den Kongress auffordert, dies gesetzlich vorzuschreiben.

Und wer glaubt, es gäbe eine freiheitsfreundliche Variante davon, der sollte sich [Sam Altmans Worldcoin](#) ansehen, das nun in „World“ umbenannt wurde. Nebenbei bemerkt: Mir fällt kein passenderer Name für diese Figur ein als „Alt-Man“.

Das [Konzept von Worldcoin](#) lautet „Proof of Human“ – eine dezentrale, datenschutzkonforme Antwort auf KI-generierte Fälschungen. Der legendäre Tech-Investor Marc Andreessen [unterstützt](#) das Projekt. Auf dem Papier könnte es sogar libertär klingen. Der Mechanismus basiert auf dem Iris-Scan. Man blickt in eine Kugel, die einem Unternehmen gehört, diese erfasst die biometrischen Daten, und man erhält eine kryptografische ID, die beweist, dass man ein Mensch ist. Es heißt, das Bild werde nicht gespeichert – lediglich ein mathematischer Hash. Doch eine aus dem eigenen Körper abgeleitete eindeutige Kennung ist ein biometrisches Merkmal, unabhängig davon, in welchem Format sie gespeichert wird.

[33 Millionen Menschen](#) haben sich bereits scannen lassen. Die App speichert nun auch von Behörden ausgestellte Ausweise. Und die Rekrutierung begann im Globalen Süden – genau dort, wo auch [MOSIP](#) (eine von der Gates-Stiftung finanzierte Plattform für digitale Identitäten) eingeführt wird. Der Einstiegspunkt ist die KI-Sicherheit. Die Infrastruktur ist dieselbe.

Aber wer baut das eigentlich auf?

Jeder in meinem Umfeld weiß, dass ich schon seit einigen Jahren vor den Gefahren von CBDC warne. Sobald sie die Komponenten verstanden hatten – programmierbares Geld, Verfallsdaten für Ersparnisse, Kontrolle darüber, was man wann kauft –, haben es manche sofort begriffen. Aber die meisten haben es einfach abgetan. Wie immer: [Bequemlichkeit statt Datenschutz](#). Keine große Sache.

Nun habt ihr gesehen, wie die Infrastruktur auf allen Kontinenten und in allen Branchen aufgebaut wird. Aber wer hat das entworfen? Mann, ich wundere mich.

Vor einigen Monaten trat Bill Gates vor die Kamera und erklärte uns das Konzept: den „Stack“ – digitale Identitätssysteme in Kombination mit digitalen Finanzschnittstellen. Er nannte die einzelnen Komponenten: MOSIP für die Identitätsverwaltung und Mojaloop für den Zahlungsverkehr. Er bezeichnete beide als „unverzichtbare Werkzeuge“ für die Zukunft, die sie gestalten. Keine zwei getrennten Dinge, sondern ein integriertes System.

Am beunruhigendsten ist vielleicht, dass der Entwurf für diesen Plan bereits vor der Krise entstand, die ihn zur Normalität werden ließ. Texte aus den kürzlich veröffentlichten Epstein-Akten zeigen [private Diskussionen](#) über die Infrastruktur für digitale Identitäten, die bis ins Jahr 2017 zurückreichen. Die Korrespondentin? Dr. Melanie Walker – Neurotechnologie-Beraterin von Gates, Direktorin bei der Weltbank, stellvertretende Direktorin der Gates-Stiftung, Beraterin der WHO und Co-Vorsitzende des [Global Future Council on Neurotechnology](#) des WEF. Sie schrieb Jeffrey Epstein eine SMS über die Schaffung „einer neuen Art von Sozialversicherungsnummer, die für alle Arten von Identitäten verwendet wird, wobei Gesundheit nur ein Anwendungsfall unter vielen ist“. [Sayer Ji](#) hat die gesamte Verbindung zur DARPA ausführlich [dokumentiert](#).

Die Strategie: „Beginne mit der Gesundheit.“ Die Vision: „Das Geniale daran ist, alle Systeme miteinander kommunizieren zu lassen.“

In denselben Texten erwähnt Walker, dass Geoff Ling von der DARPA und Raj Shah (USAID, mittlerweile bei Rockefeller) sie beide für das Amt der Surgeon General vorgeschlagen hätten. Sie erzählt Epstein, dass die Leiter des MGH, der Cleveland Clinic, von Hopkins und der Mayo-Klinik „alle zusammenarbeiten“ – und dass sie ihnen von ihm erzählt habe. Epsteins Antwort? „Setzen sie die digitale Idee bereits um? Haben sie einen Ansatz oder eine Strategie?“

Das war im Jahr 2017. Drei Jahre bevor Impfpässe das „Vorzeigen der Papiere“ für Milliarden Menschen zur täglichen Realität machten. Der Plan, der jetzt umgesetzt wird, wurde bereits Jahre zuvor von Personen, die in die Netzwerke von Gates, der Weltbank und der DARPA eingebunden waren, hinter verschlossenen Türen diskutiert – noch bevor eine Krise im Bereich der öffentlichen Gesundheit ihn politisch durchführbar machte.

[Chatham House](#), das Royal Institute of International Affairs, veröffentlichte im Januar 2024 sein Rahmenkonzept für die Regulierung globaler digitaler Plattformen. Whitney Webb hat [dokumentiert](#), wie die „Partnership Against Cybercrime“ des Weltwirtschaftsforums (WEF) dasselbe Rahmenkonzept aus der Perspektive der Cybersicherheit vorantreibt – indem sie den Internetzugang jedes Einzelnen an eine digitale ID knüpft. Die Logik ist einfach: Zustimmung durch Krisen erzeugen. Die Einstiegspunkte vermehren sich stetig, doch das Ziel bleibt immer dasselbe, ganz gleich, wer gerade an der Macht ist.

Erinnern Sie sich daran, was ich über internationale Best Practices gesagt habe? Nun, das Weiße Haus wirbt für den [SAVE Act](#) – der unter dem Deckmantel der Wahlsicherheit präsentiert wird –, indem es auf die biometrischen Wählerdatenbanken Indiens und Brasiliens als den Standard verweist, dem Amerika entsprechen sollte. Natürlich führt der Gesetzentwurf REAL ID als ersten anerkannten Nachweis der Staatsbürgerschaft auf. Der Einstiegspunkt mag hier zwar die Stimmabgabe sein, doch die Infrastruktur bleibt dieselbe.

Völlig offen

Christine Lagarde gab den [Zeitplan der EZB](#) bekannt: Pilotprojekt im Jahr 2027, vollständige Einführung bis 2029. Das ist keine Spekulation, sondern ihr erklärter Plan. Und es handelt sich nicht um eine langfristige dystopische Vision – wir stehen gerade jetzt am Scheideweg.

Sie macht kein Geheimnis aus dem Modell. Wie Efrat Fenigson [feststellte](#): „Christine Lagarde und die EZB sagen, dass China die Vorlage für ihren digitalen Euro ist. Sie kopieren den E-CNY, die digitale Währung der chinesischen Zentralbank.“ Und was erfordert das chinesische System? Eine authentifizierte Identität bei jeder Transaktion. Die Vorlage ist die Authentifizierungsebene. Das war schon immer so.

Früher war der Westen das Gegenmittel. Jetzt kopiert er die Hausaufgaben des Überwachungsstaates.

Ohne digitale Identität gibt es keine CBDC – weder in nennenswertem Umfang, noch mit Durchsetzungsfunktionen, noch als Kontrollsystem. Jede Transaktion erfordert eine authentifizierte Identität. Jede Regel muss auf jemanden angewendet werden. Die Authentifizierungsebene ist keine Komfortfunktion – sie ist der Kontrollmechanismus.

Und ja, theoretisch gibt es datenschutzfreundliche Alternativen. Aber Dinge wie Zero-Knowledge-Proofs und dezentrale Identitäten werden derzeit weder entwickelt, noch finanziert oder gesetzlich geregelt. Ganz im Gegenteil: Was derzeit eingeführt wird, ist zentralisiert, biometrisch und staatlich geprägt.

Was einmal aufgebaut ist, lässt sich nicht mehr rückgängig machen. Wann in der Geschichte der Menschheit haben die Machthaber jemals eine Machtbefugnis erlangt und diese freiwillig wieder abgegeben?

Jeder, der die Entwicklungen der letzten Jahre aufmerksam verfolgt hat, versteht, dass das, was ich hier skizziere, keine Science-Fiction ist. Kanada hat bekanntlich die Bankkonten von Lkw-Fahrern [eingefroren](#), die gegen Impfpflichten protestierten, ebenso wie die derjenigen, die für deren Sache gespendet hatten. [Chinas Sozialkreditsystem](#) schränkt bereits die Reisefreiheit von Menschen mit niedrigen Punktzahlen ein. PayPal veröffentlichte eine [Richtlinie](#), die – nach eigenem Ermessen – Geldstrafen für „Fehlinformationen“ vorsah, und zog diese erst nach heftigen Protesten zurück, wobei das Unternehmen behauptete, es habe sich um einen Fehler gehandelt. Der Mechanismus zur Bestrafung von Intoleranz blieb natürlich bestehen.

Das waren manuelle, umständliche, einmalige Eingriffe, die menschliche Entscheidungen erforderten, aber stellen Sie sich vor, all das würde automatisch, sofort und mit allem verbunden geschehen – mit Ihrem Elektroauto, der Möglichkeit Ihres Kindes, zur Schule zu gehen, sogar Ihrer Möglichkeit, sich einen Morgenkaffee zu kaufen.

Niemand nimmt dich ins Visier, niemand trifft eine Entscheidung, die Transaktion kommt einfach nicht zustande.

Und es gibt niemanden, bei dem man Einspruch einlegen könnte, da von vornherein keine Person beteiligt war.

Wenn man sehen möchte, wie der gesamte Prozess auf einer tabula rasa ohne Altsysteme implementiert aussieht, gibt es bereits ein funktionierendes Modell. Der Substack-Autor [esc](#) – meiner Meinung nach eine der derzeit wichtigsten Stimmen – [dokumentiert](#) den Wiederaufbau in Gaza außerordentlich detailliert. Der [GREAT-Trust-Plan](#) vergibt digitale Token an palästinensische Landbesitzer im Austausch gegen Landrechte – Eigentumsrechte, die in bedingten Zugriff auf einem programmierbaren Ledger umgewandelt werden. Kushner stellte in Davos [KI-gestützte Smart Cities](#) vor: sechs bis acht geplante Städte, in denen laut den Folien des Trusts alle Dienstleistungen und die Wirtschaft über ID-basierte, KI-gestützte digitale Systeme abgewickelt werden sollen. E-Wallets wurden bereits an [über 245.000 Empfänger](#) verteilt – noch bevor der Wiederaufbau überhaupt offiziell begonnen hat. Kein Bargeld. Keine Anonymität. Keine Interaktion außerhalb des Systems.

Die Architektur, die ich in diesem Aufsatz beschreibe, ist nicht theoretischer Natur. Gaza scheint das Versuchslabor zu sein. Wenn dem kein Einhalt geboten wird, vermute ich, dass wir in den kommenden Monaten und Jahren mit einem strategischen Einsatz dieser Architektur auf der ganzen Welt rechnen müssen.

Was Sie tun können

Das System benötigt Ihre Mitwirkung, um zu funktionieren.

Der Haken daran ist, dass dies gleichzeitig seine größte Schwäche sein könnte. Es wird erst dann zu einem Käfig, wenn die Akzeptanz nahezu universell ist. Mit anderen Worten: wenn ein Verzicht darauf bedeutet, dass man am täglichen Leben nicht mehr teilnehmen kann. Solange Bargeld noch funktioniert und analoge Alternativen bestehen bleiben, mag Widerstand zwar unbequem sein, ist aber noch erträglich. Deshalb brauchen sie Ihre freiwillige Mitarbeit.

Machen Sie nicht mit.

Nutzen Sie Ihren Reisepass zum Fliegen und zahlen Sie, wo immer möglich, bar. Vor allem aber: Wehren Sie sich um jeden Preis gegen die Einführung des „Real ID“-Systems. Die Verantwortlichen versuchen, Hindernisse aus dem Weg zu räumen – je mehr wir sie also durch zusätzliche Hürden aufhalten können, desto schwieriger wird es für sie, ihren Plan umzusetzen.

Für einen detaillierten praktischen Leitfaden – wie man sich in den Bereichen Bankwesen, Reisen und Alltag außerhalb des Systems zurechtfindet – verweise ich Sie auf die Arbeit, die Catherine Austin Fitts und das Solari-Team seit Jahren leisten. Sie haben intensiv daran gearbeitet, die Infrastruktur des Widerstands zu kartieren, während die meisten „Normies“ noch darüber debattieren, ob all das überhaupt real ist.

Für einen detaillierten praktischen Leitfaden – wie man sich in den Bereichen Bankwesen, Reisen und Alltag außerhalb des Systems zurechtfindet – verweise ich Sie auf die Arbeit, die [Catherine Austin Fitts und das Solari-Team](#) seit Jahren leisten. Sie haben die Infrastruktur des Widerstands kartiert, während die meisten „Normies“ noch darüber debattieren, ob all das überhaupt real war.

Wenn uns die Möglichkeit am Herzen liegt, außerhalb der Reichweite einer technokratischen Regierung zu leben – einer Regierung, die Elemente der „Cancel Culture“, von ESG und Überwachung aufgreift und sie in ein vom Staat kontrolliertes, programmierbares Währungssystem umsetzt –, dann ist dies der Kampf, für den es sich zu kämpfen lohnt. Nicht, weil wir danach jede Schlacht gewinnen werden – ich bin mir ziemlich sicher, dass wir das nicht werden. Aber wenn wir diese Schlacht verlieren, wird alles andere exponentiell schwieriger.

Sobald die Authentifizierungsebene überall etabliert ist, wird jeder andere Kontrollmechanismus lediglich zu einem Software-Update.

Der Käfig ist nicht verschlossen. Noch nicht.

Mein Freund hält die digitale ID immer noch für eine Ablenkung. Ich bin mir nicht sicher, ob ich ihn schon überzeugt habe. Aber ich bin mir auch nicht sicher, ob er sich den Luxus, sich in dieser Sache zu irren, noch lange leisten kann.

Helft ihnen nicht dabei, das System aufzubauen.