

## They're constructing the perfect beast: Who is able to make war with him?

---

[standforhealthfreedom.com/blog/beast/](https://standforhealthfreedom.com/blog/beast/)

August 2, 2023

Simultaneously on all seven continents of the world, a system is being built that will be used to surveil humanity, severely limit human freedom, and coerce and control human behavior.[1] What could possibly be the use of a system like this? How about essentially “de-banking” people when other efforts to silence their voices fall short? Joseph Mercola, his employees, *and their families*, reportedly woke up on a recent late July morning to find that their Chase bank accounts had been shut down — even their children will be prohibited from banking with Chase.[2]

This is a nightmare scenario, previously only played out in dystopian science fiction like “Minority Report.” But the declared pandemic used the leverage of fear to catapult these technologies into our homes and communities amid promises of safety.

This system is a cunningly deceptive weapon within a stealth war, the destructive power of which is impossible to underestimate. We’ve heard this drumbeat of war in the name of the “greater good” before. Now the cries are for “pandemic preparedness.”

The World Health Organization (WHO) is front and center in this so-called “Great Reset,” alongside the World Economic Forum (WEF) and the leadership of the European Commission, the “politically independent executive arm” of the European Union (EU).[3] But from within the sea of humanity, an incredibly wide variety of people and nations are participating in this work—some knowingly, some unknowingly.

According to a June 2023 WHO press release, the WHO recently launched a “landmark digital health partnership” with the EU “to establish a global system that will help facilitate global mobility and protect citizens across the world from ongoing and future health threats.”[4] The effort is called the WHO’s Global Digital Health Certification Network and represents “the first building block of digital public health infrastructure for developing a wide range of digital products for strengthening pandemic preparedness and to deliver better health for all.”[5]

## Large Scale Pilots

Prior to its roll-out in Member States the EU Digital Identity Wallet is piloted in four large scale projects, that launched on 1 April 2023. The objective of these projects is to test digital identity wallets in real-life scenarios spanning different sectors. Over 250 private companies and public authorities across 25 Member States and Norway, Iceland, and Ukraine will participate.

Eleven use cases are explored in particular:

1. **Accessing government services:** Secure access to digital public services, such as applying for a passport or driver's licence, filing taxes, or accessing social security information.
2. **Opening a bank account:** Verification of a user's identity when opening an online bank account, eliminating the need for the user to repeatedly provide their personal information
3. **SIM Registration:** Proof of identity for the purpose of pre- and post-paid SIM card contracts (registration and activation), reducing fraud and costs for mobile network operators.
4. **Mobile Driving Licence:** The storage and presentation of the mobile driving licence in both online and physical interactions such a driver providing their licence on the side of the road.
5. **Signing contracts:** Creating secure digital signatures for signing contracts online, eliminating the need for paper documents and physical signatures.
6. **Claiming Prescriptions:** Providing details of prescription to pharmacies and initiating the dispensation of medical products.
7. **Travelling:** Presenting information from travel documents (e.g. the user's passport, visa, and other), allowing for quick and easy access when going through airport security and customs.
8. **Organisational Digital Identities:** Proving you are a legitimate representative of an organisation.
9. **Payments:** Verification of a user's identity when initiating a payment online.
10. **Education certification:** Proof of possession for educational credentials, such as diplomas, degrees, and certificates making it easier to apply for jobs or further education.
11. **Accessing Social Security benefits:** An EU Digital Identity Wallet can be used to securely access a user's social security information and benefits, such as retirement or disability benefits. It can also be used to facilitate freedom of movement by storing documents such as the European Health Insurance Card.

Source: European Union Website "Shaping Europe's digital future"  
"EU Digital Identity Wallet Pilot implementation"  
<https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation>  
Screenshot taken July 26, 2023

- 
- 
- 
- 

### Health monitoring at the center of the global digital identity system

---

The WHO's publication "Global Strategy on Digital Health 2020-2025" outlines what it calls a "digital transformation of health care" that will include the use of powerful technologies such as "the Internet of things, virtual care, remote monitoring, artificial intelligence, big data analytics, blockchain, smart wearables, platforms, tools enabling data exchange, and storage and tools enabling remote data capture." [6] The WHO's global strategy "aims to create a shared understanding among all Member States regarding the importance of digital health solutions," with a digital "ecosystem" that sounds a lot like a new world wide web.

This very same “information technology infrastructure” described in the WHO publication is quoted word for word in the “United Nations September 2022 Working Group Report on AI Capacity Building – Artificial Intelligence and Digital Transformation Competencies for Civil Servants.”[7] The WEF calls this global effort the Fourth Industrial Revolution and it’s designed to connect nearly everything, and everyone, to the digital world, creating an “Internet of Things” (IoT).[8]

People themselves will be a part of the new digital ecosystem. In 2019, the United Nations produced a publication titled “Smart Cities – Shaping the Society of 2030,” describing future scenarios including a student who “walks quickly around campus through a series of automatic doors that open by detecting the digital identity chip inserted under the skin of his wrist the day he enrolled.[9] The chip also gives him access to the restaurant and allows him to borrow a bicycle and to open the door to his small room.” (Sounds eerily similar to work being undertaken at the University of Illinois, reported on by SHF in our article, “This is your warning.”)

The work to fulfill the WHO’s vision for a “digital transformation of health care” is going full throttle in the United States, despite congressional opposition and American outcry. In July 2023, a U.S. representative to the negotiations for a new pandemic treaty stated firmly on record, “The United States remains fully committed to an ambitious pandemic accord that will benefit all countries, built on practical and implementable solutions that we develop together.”[10] She would have known that digitizing health care and medical decisions is a foundation for the treaty. In fact, the current administration endorsed vaccine credentials for international travel in an agreement called the “Bali Declaration,” which you can read more about in SHF’s article “Who’s calling the shots?” Federal agencies involved with the foundational tech needed to “modernize,” and “standardize” medical coding to facilitate digital identities have been hard at work, including updating codes for tracking “underimmunization for COVID-19,” detailed in SHF’s “Z codes for medical tracking started at the WHO.”

Make no mistake: The “digital transformation of health care” is a Trojan horse of the full-spectrum control system, all revolving around the creation of “digital identities,” as mentioned in the United Nations’ paper describing the life of a student. A digital identity will be made available to *every single person in the world* as soon as 2030, with the most advanced and complex “pilot programs” currently taking place in Europe without much, if any, awareness by U.S. citizens.[11] The creation and use of a digital identity begins the process of turning a person into an IoT “node” in the new digital ecosystem. With digital identities now being pushed as a “human right,” you can see how people are to become one of the fully connected “things.”[12] And global big business and ever-increasing portions of the corporate world are completely on board. Many businesses already have detailed plans for being a part of the trillions and trillions of dollars promised by the WEF in the Fourth Industrial Revolution.[13]

#### **Deloitte Consulting: a case study in public-private partnerships for digital identities**

---

Companies like Deloitte Consulting, which unabashedly claims on its website to be “a long-standing strategic partner of the World Economic Forum (WEF)...,” has a history of also working directly with the WHO and is a major participant in the United Nations’ “Global Compact.”[14] Deloitte Consulting calls what is taking place a “new era of global public health partnerships” where “more governments are working with the United Nations, the World Bank, the World Health Organization (WHO), and other organizations...” But more governments are also working very closely with Deloitte Consulting and paying Deloitte Consulting enormous sums of money to advance the WEF’s and the WHO’s goals. Freedom of Information Act requests confirm that the state of Illinois, which under the leadership of Governor JB Pritzker led the nation in promoting tyrannical restrictions on citizens using made-up COVID-19 data, is now paying Deloitte Consulting \$53,308,797.82 for a “Public Health Digital Transformation Enablement” project scheduled to be completed no later than January 2025.[15]



# The future of government rests on the future of identity

The blending of digital and physical worlds opens up new possibilities for public services—but a new vision of identity is required to improve trust and deliver on those possibilities.

**Image Source: Deloitte Consulting Website PDF**

**"The future of government rests on the future of identity". Pg 1**

https://www2.deloitte.com/content/dam/insights/articles/us144373\_cgi\_digital-identity-pov/DI\_US144373\_Digital-identity-POV.pdf

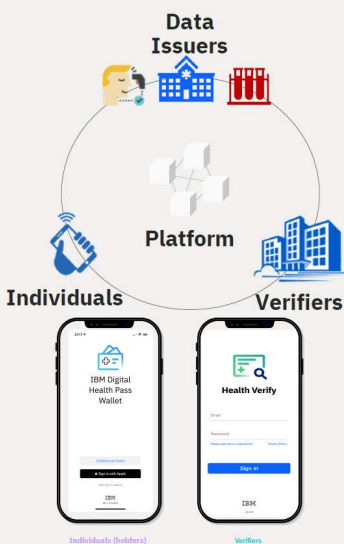
•  
•  
•  
•

While specific details of the state of Illinois' digital transformation project with Deloitte Consulting are scant, Deloitte Consulting has published countless pages on the internet outlining the mechanisms by which the global system to coerce, control, and surveil humanity will likely work, include the following titles: "The future of government rests on the future of identity", "Delivering the digital city: Building a best-in-class experience in smart cities", "Citizen Digital Identity and Digital Credentials for Re-Opening Borders, Travel, and Economies, to Return to 'Normal Life'", "Smart Cities, Smarter Public Health", "What is smart identity", "The future of digital identity — What does it mean to you?" etc.[16]

Aiding in the effort to advance the global digital identity agenda, Deloitte Consulting is also in a "long-standing strategic alliance" with International Business Machines (IBM).[17] During 2021, providing a snapshot of what is to come, the state of New York utilized and promoted IBM's health pass called the Excelsior Pass, which was "powered by IBM Digital Credentials, a blockchain-based platform that anchors digital credentials in trust and provides individuals and organizations with the core capabilities they need to securely issue, manage, and verify digital credentials." [18]

## IBM Digital Health Passport – what is it actually?

A digital credential enabling organizations to **verify** that employees, customers, visitors, contractors, etc. are **safe** to engage with each other again, while protecting their **privacy**.



1. **Individual** initiates a health activity – symptom checker app, temperature check, COVID test, vaccination, etc. and consent to share with **data issuer** (lab, gov entity, etc.)
2. **Data Issuers** create verifiable credentials and send them to **individual** wallets via platform
3. From verifiable credentials on the individual phone, a one-time health passport (or score) is created to present to a **verifier** for entry
4. **Verifier** can check the validity of the Health Passport and the association to the individual via the platform and let the **individual** in



- Back to Work
- Back to Fun
- Back to Shop
- Back to Travel
- Back to Care
- Back to School
- Back to Events
- Back to ...



Source: IBM Powerpoint Presentation: "Re-Opening States with Trust, Security and Safety - Overview of 'Digital Health Passport' A blockchain-enabled credential solution", Pg. 2, Obtained via Freedom of Information Act request, Attachment to April 10, 2021 Dept of Innovation & Technology email Subject: Fw: RE: Meeting w Gov Office

•  
•  
•  
•

### How could digital identities limit our freedom?

Digital identities are not about protecting human rights. It's easy to visualize a future where, for a person to participate in basic societal activities or even possibly receive government licensing or services, they will have to create a blockchain-based digital identity and a digital wallet, which will contain their digital credentials. It doesn't take much imagination to see how pilot programs for a convenient digital driver's license stored in their

digital wallet as part of the citizen's digital identity would become required in order to drive, similar to the way electronic transponders such as *E-ZPass* moved from an optional convenience to literally stopping travelers from using certain highway exits.[19] We've seen many examples of digital vaccine credentials, like the *GreenPass* in the U.K. or the *Excelsior Pass* in New York.

Subsequent to the creation of their digital identity, citizens will very likely be given a digital identity score or "trust score" based on how much of their personal, private information they have shared and the citizen's level of submission to the system.[20] To enable this digital identity and scoring system to operate, national and state governments, which will be among the main issuers of digital credentials, are creating enormous and seamlessly interoperable databases containing all the citizen information the government uses to collect taxes and provide licenses, permits, and services. The scope of a citizen's interaction with government, national, state, and local authorities is vastly underestimated.

As this digital identity and score system rolls out, citizens will be told that they, the citizen, have "control over their data," and that it's their individual choice "to control which credentials to use, which data they release, and to whom they release that data." [21] But what citizens will soon realize is that there will be negative consequences, such as discrimination by private-sector businesses — and even by government. They'll suffer consequences for actions like not sharing personal information or not possessing the necessary government credential, such as proof of vaccination. Here's an example: While promoting COVID-19 restrictions in 2021, Illinois Governor JB Pritzker, a proud attendee at the WEF's annual meeting in 2023, perfectly summarized how the stealth tyranny will be enforced when he said regarding proof of vaccination requirements: "As long as it is your choice." ... "If people ask you to show that for a particular venue or private venue, they have the ability and right to do that. You don't have to show that to them. You don't have to go to that venue or be engaged in that activity." [22] As more and more businesses, which may themselves be coerced by the system, demand access for citizen data, a citizen will experience more and more limitations on the activities in which they are able to participate if they are unwilling to comply with system-enabled requirements.

This becomes even more concerning when considering the financial side of the digital identity/digital wallet system, as we witnessed with Joseph Mercola. The new digital currency held within a citizen's digital wallet is also a big part of the control mechanisms of the digital identity system because software-based digital currency is "programmable" and could be used to limit how a citizen is able to spend their own money. According to Deloitte Consulting, by using programmable digital currency "a parent will be able to program a digital currency to be used only by their child and only, say, for spending on certain essentials like food and clothing but not, for example, alcohol. Programmable money may also find applications in loyalty schemes, multi-party highly manual transactions such as home buying, tax collection, and the delivery of other government services, including grants and loans," meaning that digital currency can have very, very specific limitations placed on its use.[23]

Lastly, the capture and use of a citizen's geolocation and biometric/facial recognition data will make the system nearly impossible to escape or avoid. In fact, citizens may end up having to "love," or even "worship," the system. Both governments and retailers all across the globe are installing highly sophisticated facial recognition cameras and software that is increasingly able to determine a person's emotional status.[24] According to the WEF's website, the Tunis government is working to "use human emotional recognition technology by mapping the facial expressions of citizens during their interaction with a governmental service. It uses an algorithm that allows the government to flag areas where dissatisfaction levels are higher in real time for timely interventions whenever possible." [25] Imagine being forced to "love" a system because the system itself can make your life dependent upon "loving" it. In a video titled "8 Predictions for the World in 2030," the WEF is quoted as saying: "You will own nothing. And you will be happy." [26] When this "perfect beast" system is fully built out, it's highly likely that being "happy" will be just another "choice" a citizen is "free" to make.

---

### **What can you do to plan for the best, but prepare for the worst?**

You're already taking steps to protect yourself and your loved ones by reading this article and educating yourself on what's happening. You're arming yourself with information so you can stand up for constitutional rights. If someone — whether it be a politician, religious leader, or business leader — is promoting, supporting, or advancing this system or any part of it, they are in league with the beast whether they know it or not. Call them out — privately at first, if possible, and publicly, if necessary.

Continue to shine the light of truth. Discernment of truth and the knowledge of how to navigate the system will be absolutely vital as this system expands into every aspect of daily life.

---

### **Steps you can take**

N

#### **Step One: Refuse to stay silent.**

1. Spread the word by sharing this article.
2. Join Stand for Health Freedom to stay up to date on critical developments and action items, easily shareable with a few button clicks.
3. Talk about this subject with everyone you can. Print the article and accompanying images and hang them on the bulletin board at your grocery store or church.
4. If you haven't done so already, remind your lawmakers to protect your First Amendment right to free speech by signing SHF's petition.

Sign the Petition

N

**Step Two:** Help Stand for Health Freedom help you! Please consider a donation to Stand for Health Freedom so we can continue to be a go-to resource for news and action items to help defend our U.S. Constitution and the health freedom of all Americans.  
Donate today

## References and sources

---

- [1] <https://identityreview.com/global-data-policy-database/>
- [2] <https://articles.mercola.com/sites/articles/archive/2023/07/27/chase-shuts-down-bank-accounts-at-mercola.aspx>
- [3] <https://www.who.int/publications/i/item/9789241550505>, <https://www.weforum.org/reports/reimagining-digital-id/>
- [4] <https://www.who.int/news/item/05-06-2023-the-european-commission-and-who-launch-landmark-digital-health-initiative-to-strengthen-global-health-security>
- [5] <https://www.who.int/initiatives/global-digital-health-certification-network>
- [6] <https://www.who.int/docs/default-source/documents/g4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf>
- [7] <https://unesdoc.unesco.org/ark:/48223/pf0000383325>
- [8] <https://www.lairdconnect.com/resources/blog/all-about-iot>
- [9] <https://unesdoc.unesco.org/ark:/48223/pf0000367762>
- [10] [https://apps.who.int/gb/inb/e/e\\_inb-6.html](https://apps.who.int/gb/inb/e/e_inb-6.html), INB6 video, 9:15 start. Timestamp 57:35
- [11] <https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet>, <https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation>
- [12] <https://www.youtube.com/watch?v=pL4Uc2uVO6s>
- [13] <https://www.weforum.org/press/2016/01/100-trillion-by-2025-the-digital-dividend-for-society-and-business/>
- [14] <https://www.deloitte.com/global/en/about/people/social-responsibility/deloitte-and-the-world-economic-forum.html>, <https://unglobalcompact.org/what-is-gc/participants/2821-Deloitte>
- [15] <https://www.youtube.com/watch?v=A57Wof9HgKY>, <https://doit.illinois.gov/news/procurement/proc-pcovid19-141.html>
- [16] [https://www2.deloitte.com/content/dam/insights/articles/us144373\\_cgi\\_digital-identity-pov/DI\\_US144373\\_Digital-identity-POV.pdf](https://www2.deloitte.com/content/dam/insights/articles/us144373_cgi_digital-identity-pov/DI_US144373_Digital-identity-POV.pdf), <https://www.deloitte.com/content/dam/assets-shared/legacy/docs/gx-ps-dcgi-delivering-the-digital-city.pdf>, <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-dthc-playbook-executive-summary.pdf>, [https://www2.deloitte.com/content/dam/insights/articles/pt175645\\_dim\\_smart-cities/PT175645\\_DIM.pdf](https://www2.deloitte.com/content/dam/insights/articles/pt175645_dim_smart-cities/PT175645_DIM.pdf), <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-smart-identity-print-noexp.pdf>, <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-digital-identity-what-does-it-mean-to-you.pdf>
- [17] <https://www2.deloitte.com/uk/en/pages/press-releases/archive-press-release/deloitte-and-ibm-team-to-deliver-next-generation-risk-intelligence.html>
- [18] <https://www.ibm.com/blog/opening-new-york-state-for-business-with-the-power-of-blockchain/>
- [19] <https://www.potomaclocal.com/2022/10/21/i-66-ramps-at-monument-drive-to-be-e-zpass-only/>, <https://www.cbsnews.com/philadelphia/news/new-e-zpass-only-slip-ramp-is-open-in-bucks-co/>, <https://www.cbsnews.com/philadelphia/news/costly-mistakes-for-some-drivers-on-pa-turnpike-without-e-zpass/>
- [20] <https://www.youtube.com/watch?v=j1pulhPQNM>, <https://www.ibm.com/security/digital-assets/iam/verify-adaptive-access-smartpaper/IBM%20Security%20A%20Guide%20to%20Balancing%20Digital%20Identity%20Risk%20and%20Experience%20with%20Adaptive%20Access.pdf>
- [21] <https://www2.deloitte.com/ie/en/pages/technology-media-and-telecommunications/articles/digital-consumer-trends/digital-consumer-trends-data-privacy.html>, [https://www2.deloitte.com/content/dam/insights/articles/us144373\\_cgi\\_digital-identity-pov/DI\\_US144373\\_Digital-identity-POV.pdf](https://www2.deloitte.com/content/dam/insights/articles/us144373_cgi_digital-identity-pov/DI_US144373_Digital-identity-POV.pdf)
- [22] <https://www.myjournalcourier.com/news/article/State-working-on-vaccination-proof-system-16143767.php>
- [23] <https://www2.deloitte.com/uk/en/blog/financial-services/2023/understanding-the-drivers-of-change.html>
- [24] <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-facial-recognition.pdf>
- [25] <https://www.weforum.org/projects/facial-recognition-technology>

[26] <https://m.facebook.com/worldeconomicforum/videos/10153982130966479/>