

EN

the Defender®

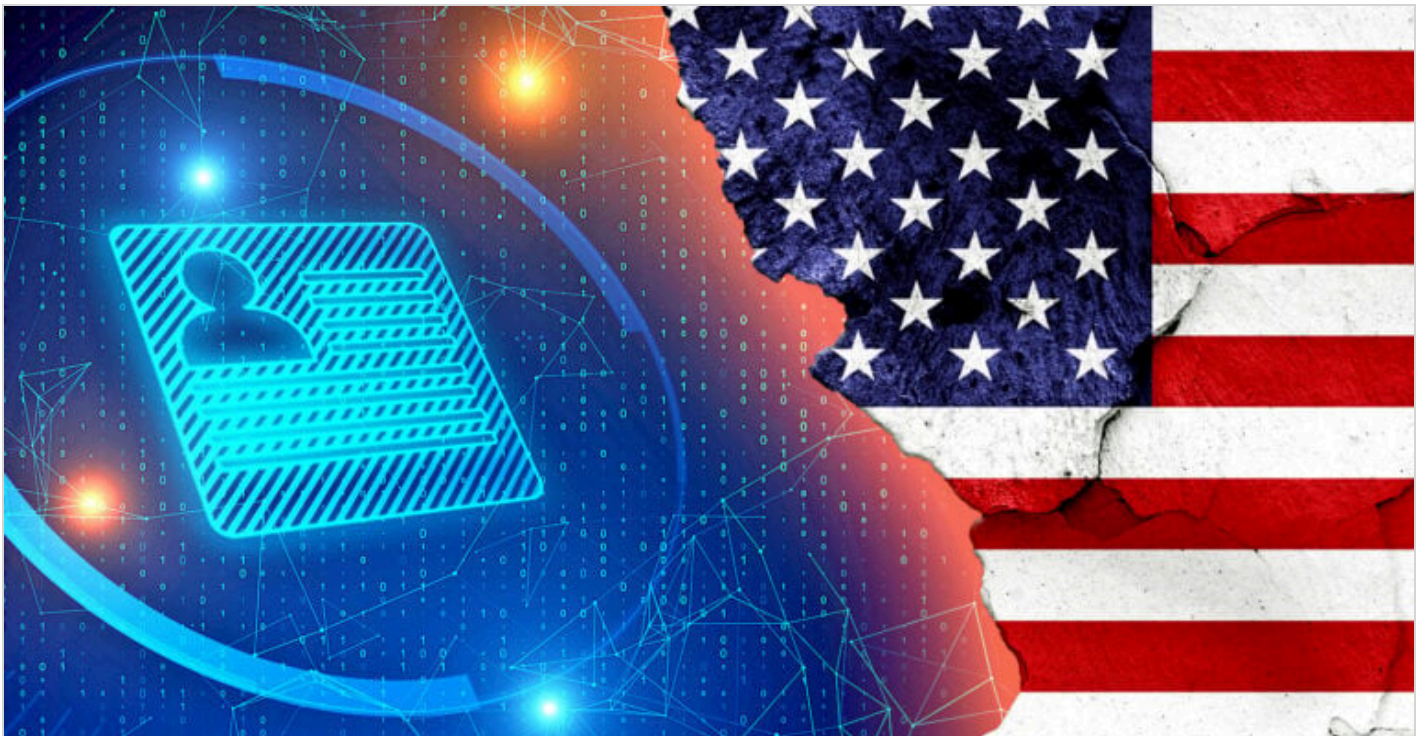
CHILDREN'S HEALTH DEFENSE NEWS & VIEWS

The Defender COVID Health Conditions Toxic Exposures Censorship/Surveillance

up the adoption of digital ID and for the development of a uniform, government-run online identity system to verify identity and age, and access public websites and services.

by Michael Nevradakis, Ph.D.

AUGUST 20, 2024



The Biden administration is drafting an executive order for federal and state governments to speed up the **adoption of digital ID** — including mobile driver's licenses — and for the development of a uniform, government-run online identity system to verify identity and age, and access public websites and services.

NOTUS, a nonprofit news outlet, obtained a draft of the executive order, which states: "It is the policy of the executive branch to strongly encourage the use of digital identity documents."

According to NOTUS, the executive order "could reshape how Americans access government services, and potentially behave online."

A digital ID system could operate with the use of biometric scans like **facial recognition** to "help better verify identity online," NOTUS reported, noting the federal government is working with Apple and Google to build systems that would "allow Americans to carry identity documents on their smartphones and frictionlessly submit them to both government and private sector websites for verification."

Michael Rectenwald, Ph.D., author of "**The Great Reset and the Struggle for Liberty: Unraveling the Global Agenda**," told The Defender that, as defined by the World Economic Forum (WEF), "**digital identity** is 'the sum total of the growing and evolving mass of information about us, our profiles and the history of our activities online.'"

Rectenwald said:

"Digital identity is not merely a new, more handy, lightweight, digital form of identification. It refers to a collection of data that purportedly defines who we are, including what we do both online and offline ... and not merely to a means by which we can be identified as such."

Alexis Hancock, director of engineering for the **Electronic Frontier Foundation**, told The Defender the Biden administration's digital ID will disproportionately target the poor and underprivileged. She said:

"Digital Identity and the standards that dictate them are still very 'new' and yet the White House is expediting digital identity for the most vulnerable of populations: people on public benefits.

"Deploying various technologies on this population to access their benefits, such as facial recognition is not something I'd encourage or advise. Especially with facial recognition being fraught with issues of discrimination."

Rectenwald also warned that digital ID can later be expanded to other functions.

“Even if a digital identity system only serves as identification at first, as the Center for Human Rights and Global Justice notes, digital identities are prone to **‘function creep’** — that is, “they are intended to be used for multiple purposes that are unforeseen when the system is first designed,” he said.

Tim Hinchliffe, editor of **The Sociable**, cited **vaccine passports** as one such possibility.

“While the federal government wasn’t able to legally mandate vaccination to all U.S. citizens, it went ahead anyway and **mandated it to federal employees**, and the **private sector** followed suit. ... The same can easily happen with digital identity,” Hinchliffe said.

The NOTUS report comes just days after revelations that the **Social Security numbers** and other personal information of practically all Americans stored by a private company, National Public Data, was breached in April 2024.

Catherine Austin Fitts, founder and publisher of the **Solari Report** and former U.S. assistant secretary of Housing and Urban Development, said, “Rather than apologize or take steps to make sure that our data is secure, the Biden administration is proposing to create even more centrally controlled databases pushing for a digital ID.”



COMING TO A
THEATER NEAR YOU
SEPTEMBER 2024

GET TICKETS

‘Big Tech manages digital ID and is far more powerful than governments’

According to NOTUS, 13 states have rolled out “some kind of mobile driver’s license program” and more are working toward implementing a digital ID. “But federal action pushing the transition has been delayed” — creating a hodgepodge of state digital ID systems that are not coordinated at the federal level.

According to **IDScan.net**, the 13 states are Arizona, California, Colorado, Delaware, Georgia, Iowa, Louisiana, Maryland, Mississippi, Missouri, New York, Ohio and Utah. **Ohio launched digital driver’s licenses** and state IDs earlier this month.

Similar programs are “in progress” in an additional 14 states, while in two states — Louisiana and Mississippi — **mobile ID can be used to vote.**

At least **seven countries have launched digital ID**, according to Identity.com. These include Canada, Estonia, Germany, India, Japan, Singapore and Sweden. The European Union (EU) **launched its digital ID and wallet** earlier this year.

Each of the 27 EU member states “will offer at least one version of the **EU Digital Identity Wallet**,” which may include driver’s licenses, personal health data, travel documents, social security information, personal SIM cards, university diplomas and also may be connected to one’s bank accounts.

In Greece, ticketing via the government’s “digital wallet” is required to **attend sporting events.**

But despite the purported convenience “digital wallets” may offer, there are also potential risks.

“If you lose your laminated driver’s license, you can just get a new one,” attorney **Greg Glaser** said. “But if you lose your biometric ID, you cannot get a new thumb or new eyeball, so hacks are permanent.”

Experts also warned of **Big Tech** involvement in government digital ID schemes. “Big Tech manages digital ID and is far more powerful than governments,” Glaser said. “Big Tech has the patents, and they dictate both the standards and implementation.”

He added:

“Their long game in the cybersecurity industry is to centralize data processing so that our state and local governments become dependent on the cybersecurity industry to function day-to-day. This is called ‘**digital public infrastructure**,’ and it is no small thing, because it neutralizes local power and governance.”

For instance, several states, including Arizona, Colorado, Georgia, Maryland and Ohio, offer their digital ID cards and driver’s licenses via Apple Wallet. Earlier this month, **Apple announced** that California will soon offer these documents via Apple Wallet as well.

According to NOTUS, although the federal government has developed Login.gov as “the standard credential for accessing federal websites,” many such sites, including that of the IRS, use “the Virginia-based start-up ID.me,” a private company.

“Through public-private partnerships, digital identity can be very convenient for citizen interactions with governments and corporations, but it can also be a tool for total surveillance and control,” Hinchliffe said.

He added:

“Just like the jabs, digital identity doesn’t have to be forcibly mandated to make your life miserable, but without it, you may not be able to make financial transactions, acquire a driver’s license, go to school or even access the internet.”



Did DOJ Lawyers Commit Fraud in the Omnibus Autism Proceeding?

LEARN MORE

According to NOTUS though, fraud involving the lack of a uniform age and identity verification system — including through state driver’s licenses that are relatively easy to forge — has cost the U.S. government billions of dollars and is a key driver of the Biden administration’s draft executive order.

“The draft order, if implemented, would ostensibly address a growing problem: The government has lost billions of dollars in **fraudulent claims** to benefit programs using forged identification cards.” Most state driver’s license systems do not connect to identity verification services that match faces to IDs.

“The result is growing interest in creating a form of digital ID to use on the web,” NOTUS reported. “Joe Biden first promised an executive order in his **2022 State of the Union address**, but it has been stuck in a bureaucratic turf war over what it should include.”

According to the draft executive order, people will not be required to submit to automated facial recognition scans. The executive order also would prohibit the government and contractors from selling biometric data and using that kind of data for anything other than identity verification.

Hancock said that while she agrees with the proposal for “more account controls for people who are at risk for fraud, like requiring multi-factor authentication and ways to recover their benefits if their credentials are compromised,” she questioned whether the White House’s proposed executive order would sufficiently address data safety.

"While there are some statements in the White House's plans that seem protective of privacy and consent in using digital identity mechanisms to combat fraud, I am wary that digital identity will lessen or mitigate fraud at scale ... This would take more robust technical support with more human aid-like useful technical support call lines and translators," she said.

Fitts said, "Digital IDs are the essential step to the WEF vision of **'Welcome to 2030**. I own nothing, have no privacy, and life has never been better."

"I do hope that with this call for digital identity, is followed by strong and robust privacy protections for our data and not naiveté that digital identity itself is the solution," Hancock said.

This article was funded by critical thinkers like you.

The Defender is 100% reader-supported. No corporate sponsors. No paywalls. Our writers and editors rely on you to fund stories like this that mainstream media won't write.

PLEASE DONATE TODAY

Establishment of CBDC the true goal of digital ID?

Experts also told The Defender that despite the Biden administration's safety assurances, government-run digital ID programs launched in other countries have been prone to breaches.

In "the process of all the data centralization ... citizens increasingly lose privacy while the authorities hypocritically claim digital wallets provide greater privacy because they are more secure against theft," Glaser said.

"The authorities' claim is at best untested and at worst outright false — as India's recent **Aadhaar security breach** showed, with about 60% of India's 1.3 billion population hacked and exposed on the dark web," Glaser said.

Aadhaar, India's national digital ID system, has been mired in **controversy**. **Promoted by Bill Gates**, Aadhaar was recently linked with **India's new digital health certificates**.

"If you want to see how digital identity gets adopted on a massive scale, take a look at India's Aadhaar digital identity system. For more than a decade, the government said that **digital identity would be voluntary**, but then banks and local governments started mandating its

use," Hinchliffe said.

This "made people's lives difficult to live without the digital ID. Now, India boasts that around 1.2 billion citizens have 'voluntarily' signed up for digital ID," Hinchliffe added.

Some experts argued that the Biden administration's true goal with digital ID is to lay the groundwork for the introduction of a **central bank digital currency** (CBDC).

"The reason that the Biden Administration wants a digital ID is so that the Federal Reserve and the banking system can move to an all-digital financial control system that will use '**programmable money**' [which] will permit taxation without representation and **negative interest rates**," Fitts said.

Similarly, Rectenwald said, "Digital identity is the lynchpin for instituting a CBDC, which the Biden administration has said in an executive order that it — and by extension, the Harris regime — intends to implement."

CBDC could be used to shut people with non-establishment opinions out of public life, Rectenwald warned. "Linked with CBDC, digital identity could bar these 'undesirables' from the economy," he said, citing people whose bank accounts were frozen for supporting or participating in the **Canadian Freedom Convoy**.



Michael Nevradakis, Ph.D.

Michael Nevradakis, Ph.D., based in Athens, Greece, is a senior reporter for The Defender and part of the rotation of hosts for CHD.TV's "Good Morning CHD."

REPUBLISH THIS ARTICLE 

SUGGEST A CORRECTION 

SHARE ARTICLE 

Get The Defender delivered to your inbox. No paywall. No ads. Just the uncensored news.