Addenda #29 – December 2024
Re: Ch. 4, The Fourth Industrial Revolution
Re: Addenda #15 – January 2024: *Digital Identities / Government Abuse of Power*

- *Digital Identities*

"We help stakeholders harness the full potential of technological progress for the equitable and human-centered transformation of industries, economies and societies"
World Economic Forum 'Centre for the Fourth Industrial Revolution' web page

A "digital identity" refers to the personal information collected by computer systems about a person over time. This information is grouped into two broad categories: digital attributes, and digital 'activities'
Digital attributes include date of birth, email address, ID numbers (social security, driver's license, passport), bank & financial details, medical information, login credentials and medical history.
Digital activities include emails and text messages, social media activity (likes, comments, posts, status updates, photos and videos posted), online searches (including maps and directions) and purchase history, signed petitions, downloaded apps and programs, and cell phone usage. This is also referred to as your "digital footprint"
All of this data used by itself or combined together can be used to identify you. It is your 'digital identity'.

As far back as 2013, the World Economic Forum was working with financial service companies to explore the way that new technologies including online and mobile banking, cryptocurrency, data analysis and Artificial Intelligence might be used interact with their customers. Financial services firm Deloitte Consulting LLP, global banks, payment card firms, financial service and equity investment firms worked with the World Economic Forum over a period of five years to identify emerging trends that would lead to new ways of doing business in the future.

In June 2015, The World Economic Forum published the results of this collaboration in a report titled, *The Future of Financial Services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed.*
The very first section of the "Key Findings" section of the report, dealt with how new technologies would affect payment systems customers use.
New consumer functionalities are being built on existing payment systems and will result in meaningful changes in customer behaviour

Implications for Financial Institutions
- *Financial institutions may lose control over their customers' transaction experience as payments become more integrated*

All of the financial institutions were concerned about losing customers as new methods of payment, digital transactions, digital wallets and P2P (Peer-to-Peer) networks would draw customers away from the traditional service that banks offer. The industry would have to change, offer reasons and strong incentives to switch to new technologies *and* retain customers. Making the switch to digital, cashless transactions would be a major push for banks and businesses. Also prominent in the list of innovations was the use of mobile payments (via smart phone technology) and mobile shopping, ordering and payment apps.

Security concerns, potential fraud and identity theft, with the use of cashless and mobile transactions, were addressed by the use of biometrics and location-based identification. Biometrics are distinct characteristics used to identify individuals. New technology could use your fingerprint to unlock your phone or access an ATM. Retinal scan readers could ensure accurate identification in a healthcare environment or unlock doors for access to high security banking facilities, military and government facilities. Facial recognition scans would allow TSA to check people in through airport security, replace boarding passes on cruise ships, or replace passports at border crossings.

As with any technology, geolocation, fingerprinting, retinal scans and facial recognition technologies can be useful, or they can be an invasion of and elimination of your privacy.

- *Government Abuse of Technology*

China is an example of how the government can take a technology like *facial recognition* and use a network of surveillance cameras to monitor its citizens. In March 2018 the *People's Daily, China*, the official newspaper of the Chinese Communist Party, claimed on Twitter: "Sky Net, a facial recognition system that can scan China's population of about 1.4 billion people in a second, is being used in 16 Chinese cities and provinces to help police crack down on criminals and improve security."
Note: The Chinese central government began building its Sky Net surveillance network system in 2005 and now has an estimated 700 million CCTV cameras in use, providing constant surveillance of the public.

German journalist Kai Strittmatter wrote the book *We Have Been Harmonized – Life in China's Surveillance State*, based on his 30-plus-year study of that country. "It doesn't even matter whether it's true or not, as long as people believe it," Strittmatter says. "What the Communist Party is doing with all this high-tech surveillance technology now is they're trying to internalize control. ... Once you believe it's true, it's like you don't even need the policemen at the corner anymore, because you're becoming your own policeman." Facial recognition technology programs collect millions of GPS coordinates through the Sky Net camera system, noting the locations of millions of Chinese residents. System databases then match faces to names, government ID numbers, addresses, photos and employers.

It's not surprising that India, North Korea, Iran and Russia are also using mass surveillance of its citizens to monitor and control their actions. But there are other countries that use surveillance technologies to monitor their citizens as well.

Canada's Communications Security Establishment (CSE) metadata surveillance program has been collecting information from telephone and internet communications for decades, establishing 'digital identities' of anyone using the internet or telephones & cellphones. (Reference: Ch. 4 The Fourth Industrial Revolution)

Australia's mass surveillance is done through telephone, internet activity and other communications providers, financial transactions, and utility records. The Australian Security Intelligence Organization has broad authority for hacking, detention and interrogation of citizens under the excuse of fighting terrorism and national security.

The United Kingdom's "bulk interception" policy collects and stores information from electronic communications like telephone calls and emails, on millions of citizens and residents. In 2021 the European Court of Human Rights ruled that this policy was a violation of human rights. Although the British government has admitted to the violations, the bulk interception policy is still in effect.

The United States conducts "domestic surveillance" through the National Security Agency (NSA). Mass surveillance in the U.S. escalated after the September 2001 terrorist attacks, with the passage of the 2001 USA Patriot Act and the 2008 Foreign Intelligence Surveillance (FISA) Act. Under Section 702 of the FISA Act, the U.S. government has engaged in mass, warrantless surveillance of Americans' and foreigners' phone calls, text messages, emails, and other electronic communications.

The NSA has a massive database of American's phone calls, which was brought to the attention of the public in 2013, by whistleblower Edward Snowdon. (Snowden also blew the whistle on Canada's CSE) The NSA operates a web of spy programs that allowed it to intercept internet and telephone conversations of Americans without specific warrants. In 2013, the U.S. FISA Court issued an order to Verizon to turn over all phone records to the NSA daily. AT&T and Sprint complied voluntarily to also turn over records of their customers. It should come as no surprise that U.S. intelligence leaders who publicly defended the program, lied to Congress and the American public. The Central Intelligence Agency also has a bulk data collection that has been hidden from the public and Congress for decades.

A 2023 report by NBC News showed that the FBI searched a foreign intelligence database for information more than 278,000 times in 2020 and 2021. The searches included Americans who participated in the George Floyd protests and the January 6 Capital Riot.

Note: A U.S. Court of Appeals found the program unlawful and a violation of Constitutional rights in 2020.

Note: President Biden signed legislation approved by the Senate in April, extending the FISA Act for another two years.

This all goes to show that U.S. law enforcement agencies and the federal government cannot be trusted to keep our personal information secure and not violate our rights!

The World Economic Forum report, *A Blueprint for Digital Identity*, goes on to state that "The need for digital identity is becoming increasingly pressing" and notes the various "solution's" private businesses, industries and governments can provide through the use of digital identities.
Global technology companies such as Google and Microsoft, will "act as platforms to authenticate users" to providers of services.
Private Service Providers will "focus on collecting the attributes they themselves need to provide specific services to users."
Governments will "focus on the provision of identity to their citizens, and providing citizens with services based on these attributes."
It sounds like the World Economic Forum and all who collaborated in this study have everything figured out. They'll provide us with a unique individual digital identity, authenticate our identity to other businesses, and collect personal data provide services to us based on our digital identities.

Kinda takes the individual choice and decision making out of the process, right? Under the World Economic Forums Digital Identity system, we will all become compliant robots, guided by the system in all of our wants and needs, and the government will know everything about us!

- *Digital Identity in the U.S.*

Financial and technology companies have been pushing for a digital identity system in the U.S. since the 2013 collaboration with the World Economic Forum I previously noted. Over the past five years, there has been a significant increase in large-scale data breaches, resulting in the personal information of consumers made available for sale on the "dark web." The availability of personal information requires an increased effort in verifying identities for online transactions, leading to more calls for a more secure system of protecting and proving the identities of individuals.

In September 2020, the bipartisan "Improving Digital Identity Act of 2020" was introduced in Congress. The purpose of the bill was to create a task force to "establish a government wide approach to improving digital identity, and for other purposes." The task force was to look into setting up a process on how to verify the identity of individuals who accesses services online or electronically and promoting digital identity credentials (e.g., electronic driver's licenses and birth certificates) for use in the public and private sectors. The bill died in the 116th Congress, never being brought to the floor for a vote. The bill was re-introduced in the next two sessions of Congress but has yet to come to the floor of either House for a vote.

In March 2023, President Biden introduced a $1.6 billion Pandemic Anti-Fraud proposal to "investigate, prosecute, and recover money from those who were engaged in major or sophisticated fraud" of pandemic stimulus programs. The Fraud Prevention and Recovery

Act was introduced in Congress in April 2024. This legislation, besides targeting pandemic fraud, authorized federal agencies like the Social Security Administration, U.S. Treasury, and the General Services Administration, to create a nationwide database to help with identity verification, and to build an "electronic verification system" that would replace paper documents and identification cards.

The lobbying group *Better Identity Coalition* has given more than $350,000 to policymakers in an effort to promote digital identification over the past six years, including supporting *Improving Digital Identity Act* legislation and emphasizing the need for a national digital identity policy. The *FIDO* [Fast Identity Online] *Alliance,* an association supported by financial, technology and other business groups, promotes biometric methods of identification to replace existing ID cards, usernames and passwords.

In January 2020, the World Economic Forum collaborated with the FIDO Alliance on a report titled "Passwordless Authentication" in which the WEF promoted using FIDO's biometric principles for identification. The report touted the many benefits of biometric identification including lower costs for businesses (lower costs associated with password management and data breaches), higher revenues for businesses (increased productivity of workers not having to take time to enter usernames and passwords), more secure transactions and "seamless" transactions.
Of course, this new "user friendly experience" would come at a cost to the customer (and a revenue to businesses), which the report justified by saying, "… experience will be more important than price. 86% of customers are indeed ready to pay a premium for more user-friendly experience." Sounds like big businesses will make out very well with this new system, and customers will pay more for it.

Another section of the WEF/FIDO report had to do with "behavioural authentication." *Behavioral biometrics* are unique behavioral traits that are tied to individual customers. Behavioral biometrics can be used to verify identity and track fraud patterns based on users' past behavior. Web sites you have visited, purchases you have made (gun purchases?), your financial transactions and accounts, your medical history (are you vaccinated?), your utility records (what is your *carbon footprint*?), and your social media history (political leanings?) all combine to make up your behavioral biometrics and your digital identity.

This is all part of the Global Elites push for coercing, or otherwise manipulating people into giving up their anonymity and freedom under the premise of better security and user-friendly experiences. Behavioral biometrics and digital identities consist of everything that makes you a unique and individual person. It consolidates all of your habits and most personal data into one record, accessible by big businesses and the government. A Public-Private Partnership. If your digital identity can be used to determine which product and services can be provided to you, it can also be used to deny you those same products and services.
"This digital identity determines what products, services and information we can access – or, conversely, what is closed off to us"
World Economic Forum, Identity in a Digital World - A new chapter in the social contract, September 2018

➢ *Final Thoughts*

The creation of a digital identity for citizens of the United States is a dangerous idea. Our elected leaders who have been proposing a task force to create a digital identity are either naïve, misguided, or complicit in creating a comprehensive database containing all our activities and attributes, our digital identity, that will be accessible to big corporations and federal agencies.

Having a Digital Identity has nothing to do with providing user-friendly seamless transactions or making access to public services easier and more inclusive.
It has nothing to do with "providing efficient, effective and seamless services to users."
It has nothing to do with verifying consumer identities or protecting our most sensitive personal information.

It has everything to do with a big, global government having all the information they need at their fingertips, to monitor and *control* its citizens.

Welcome To 2030: I Own Nothing, Have No Privacy And Life Has Never Been Better

Reference Material:
1. A Clear and Present Danger, Threat #3 – The Great Reset
2. Ch. 4 Digital Identities and the Social Credit System
3. Ch. 7 Environmental, Social and Governance (ESG) scoring; A Clear and Present Danger, Threat #2 – U.N. Agenda 21 / 2030
4. Ch. 15 Sustainable Living – Smart Cities, Smart Thermostats; A Clear and Present Danger, Threat #2 – U.N. Agenda 21 / 2030
5. 'The Future of Financial Services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed'; World Economic Forum report, June 2015
6. 'We Have Been Harmonized – Life in China's Surveillance State'; Kai Strittmatter, 2020
7. 'A Blueprint for Digital Identity - The Role of Financial Institutions in Building Digital Identity'; World Economic Forum, August 2016
8. 'Passwordless Authentication – The next breakthrough in secure digital transformation'; World Economic Forum, January 2020
9. 'Behavioral Biometrics'; International Biometrics + Identity Association White Paper, May 2017
10. 'Pulling Back the Curtain on Canada's Mass Surveillance Programs – Part One: A Decade of Secret Spy Hearings'; British Columbia Civil Liberties Association, December 14, 2022
11. FAQ: What You Need to Know About the NSA's Surveillance Programs; ProPublica, August 5, 2013
12. Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress; ACLU Commentary, April 11, 2023
13. Biden signs reauthorization of surveillance program into law despite privacy concerns; npr, April 20, 2024
14. Improving Digital Identity Act of 2020, H.R. 8215
15. Improving Digital Identity Act of 2021, H.R. 4258
16. Improving Digital Identity Act of 2022, S. 4528
17. Improving Digital Identity Act of 2023, S. 884