Technocracy Rising: The Trojan Bear Of Global Transformation

Yes, this is a play on words from the title of my 2014 book, [Technocracy Rising: The Trojan Horse of Global Transformation,](#) but it fits perfectly.

With the coronavirus as a trigger, the entirety of global equity markets have now entered a bear market, down 20% from their very recent peaks. The financial shock of peeling off up to $30 trillion of dollars in equity has barely been felt yet, but analysts are already warning of major structural faults that could turn out to be existential to the current global financial and economic systems.

In other words, the collapse of the existing economic system would leave a vacuum that would eventually have to be filled, but the big question is, filled with what?

Technocrats are standing by to answer that question: Sustainable

Development, aka Technocracy. Sustainable Development is the United Nations' version of Technocracy, which was originally defined as a resource-based economic system dependent on total control over resources, production and consumption and where energy is the primary currency. The concepts of supply and demand are jettisoned and with everything being priced according to the energy that went into its manufacturing.

For all those who think this is a foolishness, consider that this is exactly what the so-called Green New Deal ideology is all about. Thanks to the persistent encouragement by the United Nations, the color 'green' has already been imprinted on every nation on earth.

When all these green thinkers are presented with this vacuum of collapsed Capitalism and Free Enterprise, what do you think they are going to demand? A rebuilding of the same system?

Hardly. They will instead blame Capitalism and Free Enterprise as getting what it deserved for 'destroying' the world in the first place. After all, they believe it was the engine of man's exacerbation of global warming. Capitalism will become a pariah and demands for something 'new' will be shouted from the housetops (and skyscrapers).

The resulting economic fallout from the current global meltdown will see governments and central banks dishing out boatloads of fresh taxpayer-provided stimulus funding to recover from the downward spiral. Watch where the money is spent. It will be for 'green jobs', green infrastructure and other sustainable development projects.

Just as 9/11 brought the total surveillance state into existence, the coronavirus will usher in a new economic system. While that is taking place, the total surveillance state will be further reinforced by spending on Internet of Things, social engineering projects, geospatial intelligence, etc.

The lyrics of Bob Dylan's well-known ballad also fits perfectly: ***The Times They Are a-Changin':***

The line it is drawn

The curse it is cast
The slow one now
Will later be fast
As the present now
Will later be past
The order is rapidly fadin'
And the first one now
Will later be last
For the times they are a-changin'

'Geofence' Warrant Traps Innocent Bike Rider At Scene Of Crime

Police can now get warrants to demand that Google give up 'geofence' records of everyone who was near the scene of a crime. Being at the wrong place at the wrong time can get you busted as a suspect and

The email arrived on a Tuesday afternoon in January, startling Zachary McCoy as he prepared to leave for his job at a restaurant in Gainesville, Florida.

It was from Google's legal investigations support team, writing to let him know that local police had demanded information related to his Google account. The company said it would release the data unless he went to court and tried to block it. He had just seven days.

"I was hit with a really deep fear," McCoy, 30, recalled, even though he couldn't think of anything he'd done wrong. He had an Android phone, which was linked to his Google account, and, like millions of other Americans, he used an assortment of Google products, including Gmail and YouTube. Now police seemingly wanted access to all of it.

"I didn't know what it was about, but I knew the police wanted to get something from me," McCoy said in a recent interview. "I was afraid I was going to get charged with something, I don't know what."

There was one clue.

In the notice from Google was a case number. McCoy searched for it on the Gainesville Police Department's website, and found a one-page investigation report on the burglary of an elderly woman's home 10 months earlier. The crime had occurred less than a mile from the home that McCoy, who had recently earned an associate degree in computer programming, shared with two others.

Now McCoy was even more panicked and confused. He knew he had nothing to do with the break-in – he'd never even been to the victim's house – and didn't know anyone who might have. And he didn't have much time to prove it.

McCoy worried that going straight to police would lead to his arrest. So he went to his parents' home in St. Augustine, where, over dinner, he told them what was happening. They agreed to dip into their savings to pay for a lawyer.

The lawyer, Caleb Kenyon, dug around and learned that the notice had been prompted by a "geofence warrant," a police surveillance tool that casts a virtual dragnet over crime scenes, sweeping up Google location data — drawn from users' GPS, Bluetooth, Wi-Fi and cellular connections — from everyone nearby.

The warrants, [which have increased dramatically in the past two years](#), can help police find potential suspects when they have no leads. They also scoop up data from people who have nothing to do with the crime, often without their knowing – which Google itself has described as ["a significant incursion on privacy."](#)

Still confused – and very worried – McCoy examined his phone. An avid biker, he used an exercise-tracking app, RunKeeper, to record his rides. The app relied on his phone's location services, which fed his movements to Google. He looked up his route on the day of the March 29, 2019, burglary and saw that he had passed the victim's house three times within an hour, part of his frequent loops through his neighborhood, he said.

"It was a nightmare scenario," McCoy recalled. "I was using an app to see how many miles I rode my bike and now it was putting me at the scene of the crime. And I was the lead suspect."

A powerful new tool

The victim was a 97-year-old woman who told police she was missing several pieces of jewelry, including an engagement ring, worth more than $2,000. Four days after she reported the crime, Gainesville police, looking for leads, went to an Alachua County judge with the warrant for Google.

In it, they demanded records of all devices using Google services that had been near the woman's home when the burglary was thought to have taken place. The first batch of data would not include any identifying information. Police would sift through it for devices that seemed suspicious and ask Google for the names of their users.

Kenyon said police told him that they became particularly interested in

McCoy's device after reviewing the first batch of anonymized data. They didn't know the identity of the device's owner, so they returned to Google to ask for more information.

[Read full story here…](#)
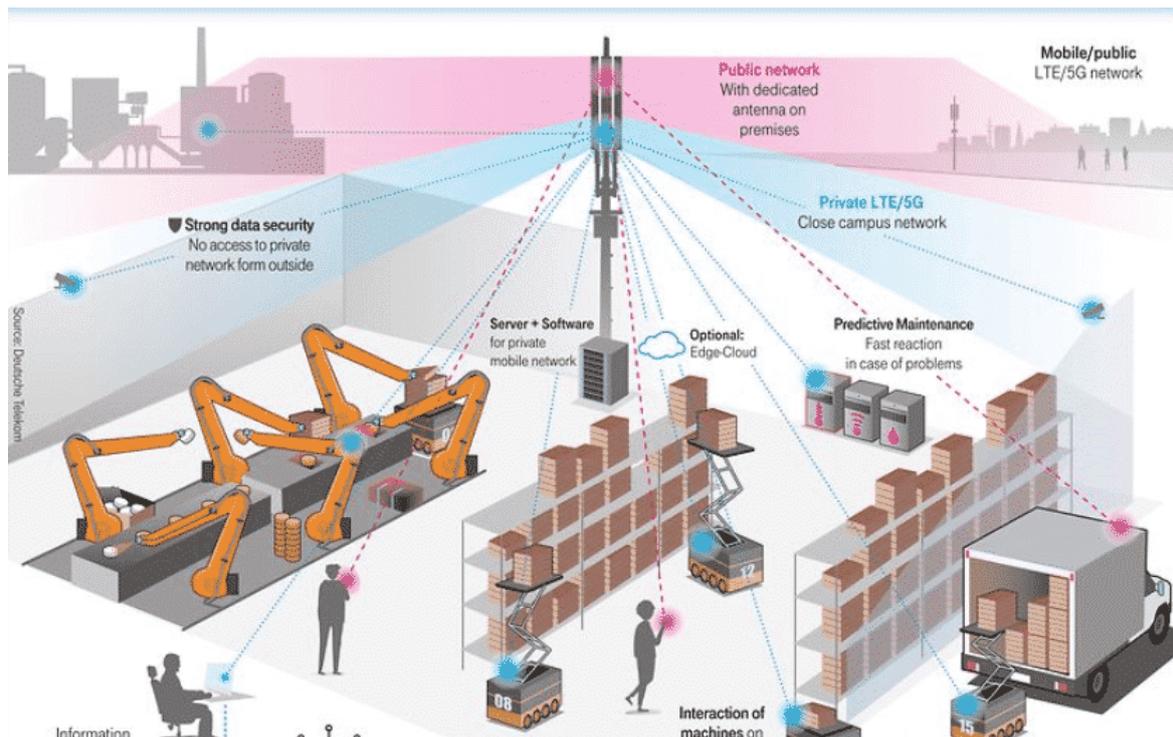
T-Mobile: IoT And 'The Transformative Promise Of 5G'

T-Mobile paid to have this article appear on the CNBC website, and you can read for yourself that 5G is all about the IoT and tracking things that move. T-Mobile's 5G network will operate at the ultra-high frequency of 600MHz. ⁘ TN Editor

The 5G future of networking promises high speeds, low latency and plenty of bandwidth to support concurrent connections, all of which will be transformative. But the excitement over this next-gen tech is about more than a speed or capacity bump. The 5G era has the potential to radically transform the way we think about and use mobile networks and

networks in general.

The networks of the future need to carry enhanced mobile broadband, a far greater volume of machine-to-machine communications to support the Internet of Things for both consumer and industrial applications, and the mission-critical business traffic that will enable Industry 4.0. And to support global business supply chains, these networks need to enable seamless communications worldwide.

The concept of a 5G campus network could meet the needs of smart manufacturing facilities with heavy utilization of the Industrial Internet of Things (IIoT) and specific tailoring for the demands of the digital economy, including enhanced data security, careful attention to customer experiences and digital logistics.

The architecture of a campus network involves a "dual slice" solution: two slices being broadcasted — a public network (the "public slice") and an exclusive private network (the "private slice") — running on the same hardware. Superficially, this resembles the commonplace setup of a business using a WLAN for data exchange, such as industrial purposes, while employees and customers connect to carrier 4G/LTE networks for their personal communications. But the implications are very different and wide ranging.

For one thing, the campus network marks a radical shift towards mobility. Instead of having a network supplier provide infrastructure and a mobile network operator providing the cellular network from the outside, the mobile network operator is both the provider for smartphone data and the enterprise network at the core of the system.

Today, a company's wireless network infrastructure — the equivalent of a "private network" — is Wi-Fi. Outside of a company facility, employees' mobile devices run on a carrier's 4G/LTE network. Of course, switching between Wi-Fi and mobile networks can happen automatically on employees' smartphones. But what about a robot? Or a pallet full of goods that you need to track as it leaves a facility, during its journey in a shipping container, and as it arrives at a distribution warehouse?

That's where the advantage of a campus network — especially in a 5G

era world — is clear. As 5G becomes common virtually everywhere, having a single network protocol to think about can greatly simplify operations. And with a growing opportunity to develop and deploy 5G radios that can operate within the unlicensed spectrum currently used by Wi-Fi, as well as on licensed bands allocated to carriers regionally, companies may not need to worry about national boundaries. Think of it as a sea of carrier coverage, within which are islands of private coverage, with seamless roaming between them.

This opens up tremendous possibilities for scaling machine-to-machine communication and manufacturing mobility. And today's private campus networks — those "islands" — are both a step towards and a laboratory for experimentation with future public 5G services.

One concept Deutsche Telekom is currently piloting is the delivery of a campus network as a service (NaaS). In this use case, a wireless carrier supplies and maintains the infrastructure, delivering a private slice serving the client's mission-critical needs while also giving the client use of the carrier's public slice for other purposes. In a large campus installation — an airport, seaport or industrial park — multiple private slices could exist and scale as needed, with clients using portions of carrier spectrum or purchasing rights to specific frequencies in a given geographic area as needed.

And that scalability is the key to making NaaS more than a business model. The advantage for customers is flexibility. Delivering the network as a service will eventually provide the same elasticity that cloud computing does — a customer can get a certain base amount of capacity and have access to overflow if they need it.

As part of another pilot, Deutsche Telekom demonstrated the strengths of the concept in the context of a large-scale test implemented at the Port of Hamburg, with multiple network slices flexibly adapted to suit specific needs over time. Individual virtual networks were spun up to serve public mobile access, emergency services, sensors for real-time analysis of environmental data and a high-bandwidth network to support the testing of augmented reality services for maintenance workers. Another test installation by Deutsche Telekom, at a light manufacturing

plant in Schwabmünchen, Germany, focused on IoT applications, including automated, guided vehicles.

While the first large-scale national rollouts of 5G service are just appearing this year (T-Mobile launched its 5G network on existing 600 MHz spectrum nationwide on December 2, 2019), the biggest implementations are set to come online over the next few years. The implementation of pilot private networks on manufacturing campuses gives us a chance to see the future in action right now: faster, yes, but more flexible, more connected and more mobile than ever before.

[Read full story here...](#)