MERCOLA
Take Control of Your Health

# The End of Privacy Is Near

Analysis by Dr. Joseph Mercola | November 17, 2023

## STORY AT-A-GLANCE

- "CITIZENFOUR" is a documentary about NSA whistleblower Edward Snowden. It came out in 2014, but it's even more pertinent today than it was then
- In January 2013, when documentary film director/producer Laura Poitras received an encrypted email from a stranger who called himself "Citizen Four"
- In June 2013, Poitras flew to meet Snowden at the Mira Hotel in Hong Kong, together with columnist Glenn Greenwald and Guardian intelligence reporter Ewen MacAskill. After four days of interviews, Snowden's identity was made public at his request
- Today, Snowden's warnings ring truer than ever. Artificial intelligence now scours social media, podcasts and videos for key words identifying "anti-vaxxers," for example. It doesn't even matter if they agree with what you're writing or saying. The mere inclusion of certain words will get you axed from the platform
- Next, the plan is to eliminate privacy altogether by requiring a digital identity to access the internet

"CITIZENFOUR" is a documentary about U.S. National Security Agency (NSA) whistleblower Edward Snowden. It came out in 2014, but it's even more pertinent today than it was then, so if you haven't seen it, I urge you to do so.

The Snowden story began in January 2013, when documentary film director/producer Laura Poitras received an encrypted email from a stranger who called himself "Citizen

Four." Snowden reportedly chose this codename "as a nod to three NSA whistleblowers who came before him: Bill Binney, J. Kirk Wiebe and Thomas Drake."

Poitras had already spent several years working on a film about monitoring programs in the U.S., and had been placed on a secret watch list after her 2006 film "My Country, My Country,"[1] a documentary about Iraqis living under U.S. occupation. In his initial email, Snowden wrote:

> *"Laura. At this stage, I can offer nothing more than my word. I'm a senior government employee in the intelligence community. I hope you understand that contacting you is extremely high risk and you're willing to agree to the following precautions before I share more. This will not be a waste of your time ...*
>
> *The surveillance you've experienced means you've been 'selected' — a term which will mean more to you as you learn about how the modern SIGINT system works.*
>
> *For now, know that every border you cross, every purchase you make, every call you dial, every cell phone tower you pass, friend you keep, article you write, site you visit, subject line you type, and packet your route, is in the hands of a system whose reach is unlimited, but whose safeguards are not.*
>
> *Your victimization by the NSA system means that you're well aware of the threat that unrestricted secret police pose for democracies. This is a story few but you can tell."*

## Summary of Snowden's Journey

In June 2013, Poitras flew to meet Snowden at The Mira Hong Kong, together with columnist Glenn Greenwald and Ewen MacAskill, an intelligence reporter for The Guardian. After four days of interviews, Snowden's identity was made public at his request.

Within two weeks, the U.S. government demanded Snowden's extradition. Facing prosecution in the United States, Snowden scheduled a meeting with the United Nations High Commissioner for Refugees and applied for refugee status.

He managed to depart Hong Kong, but became stranded at the Sheremetyevo International Airport in Moscow when his passport was canceled. There he remained for 40 days, until the Russian government finally granted him asylum.

## The Greatest Weapon of Oppression Ever Built

The U.S. government implemented Stellar Wind, a program to actively — and illegally — spy on all Americans within days of the 2001 9/11 attack. Ten years later, in 2011, construction began on a NSA data center in the Utah desert. It's now the largest surveillance storehouse in the U.S.

In his correspondence, Snowden warned Poitras that "telecommunication companies in the U.S. are betraying the trust of their customers." Through Stellar Wind, all phone calls and text messages were being intercepted and stored, and the Stellar Wind program has only expanded from there.

The NSA not only intercepts American citizens emails, phone conversations and text messages, but also Google searches, Amazon.com orders, bank records and more.

> *"We are building the greatest weapon for oppression in the history of man,"* Snowden wrote, *"yet its directors exempt themselves from accountability ... On cyber operations, the government's public position is that we still lack a policy framework. This ... was a lie.*
>
> *There is a detailed policy framework, a kind of martial law for cyber operations created by the White House. It's called 'Presidential Policy Directive 20' and was finalized at the end of last year."*

## Linkability, the Key to Control — and Entrapment

As explained in the film, a key aspect of control through surveillance is the linkability of data. One piece of data about you is linked to another piece. For example, your bus pass can be linked to the debit card you used to buy the pass. Your debit card is also linked to all other purchases.

With two key pieces of information — WHERE you went on a given day, and WHEN you made purchases, they can determine who you spoke with and met up with by linking those data points with those of other people who were in the vicinity at the same time. And that's without even using your cellphone data.

When all these various data points are aggregated — location data, purchases, phone calls, texts, social media posts and more — you end up with a collection of metadata that tells a story about you. However, while the story is made up of facts, it's not necessarily true.

For example, just because you were standing at a particular street corner does not mean you had anything to do with the crime that was reported on that same corner at the time you happened to be there. The problem is, your data could be used against you in that way.

The January 6 prisoners are a perfect example of how bits and pieces of data can be misused. Many have now spent years in jail simply because their cellphone data showed them as being in the wrong place at the wrong time.

## State Power Versus the People's Power to Oppose That Power

When asked by Greenwald why he decided to become a whistleblower, Snowden replied:

> *"It all comes down to state power against the people's ability to meaningfully oppose that power. I'm sitting there every day, getting paid to design methods to amplify that state power.*
>
> *And I'm realizing that if the policy switches that are the only thing that restrain these states were changed, you couldn't meaningfully oppose [them].*

*I mean, you would have to be the most incredibly sophisticated tactical actor in existence. I'm not sure there's anybody, no matter how gifted you are, who could oppose all of the offices and all the bright people, even all the mediocre people out there with all of their tools and all their capabilities.*

*And as I saw the promise of the Obama administration be betrayed ... and in fact, [how they] actually advanced the things that had been promised to be sort of curtailed and reined in and dialed back ... As as I saw that, that really hardened me to action ...*

*We all have a stake in this. This is our country, and the balance of power between the citizenry and the government is becoming that of the ruling and the ruled, as opposed to the elected and the electorate."*

## A Decade Later Snowden's Words Ring Truer Than Ever

"I remember what the internet was like, before it was being watched, and there's never been anything in the history of man like it," Snowden said.

*"You could have children from one part of the world having an equal discussion, where they were sort of granted the same respect for their ideas and conversation, with experts in a field from another part of the world on any topic, anywhere, anytime, all the time.*

*It was free and unrestrained. And we've seen the chilling of that, and the changing of that model towards something in which people self police their own views. They literally make jokes about ending up on 'the list' if they donate to a political cause, or if they say something in a discussion. It's become an expectation that we're being watched.*

*Many people I've talked to have mentioned that they're careful about what they type into search engines, because they know that it's being recorded, and that limits the boundaries of their intellectual exploration."*

Today, after the extreme ramp-up of censorship, surveillance and harassment we've endured since the COVID pandemic began, Snowden's warnings ring truer than ever.

Artificial intelligence now scours social media, podcasts and videos for key words identifying "anti-vaxxers," for example. It doesn't even matter if they agree with what you're writing or saying. The mere inclusion of certain words will get you axed from the platform.

Snowden's worst fears have indeed come true, and today most people have come to realize just how dangerous this kind of blanket surveillance can be. Countless individuals whose only "crime" was to share their story of how the COVID shot ruined their lives have had their posts censored and social media accounts shut down.

Canadians whose only "crime" was to donate a few dollars to a peaceful protest had their bank accounts frozen. Small companies and nonprofit organizations with the "wrong" viewpoints have had their online payment services cancelled, effectively strangling their ability to make a living and keep the operation going.

Others have been debanked without recourse, including yours truly. My CEO and CFO and all of their family members also had their accounts and credit cards canceled, apparently for no other reason than the fact that they work for me. In other words, guilt by association.

## Will the Internet as We Know It Disappear in the Next Year?

I recently posted an **interview with investigative journalist Whitney Webb** in which she talks about the next steps in the ramp-up of tyranny. The World Economic Forum has warned we may face a cyberattack on the banks before the end of 2024. That means we almost definitely will, seeing how they like to announce plans ahead of time.

Such a cyberattack will not only destroy the current banking system and usher in programmable central bank digital currencies. It will also eliminate privacy online by requiring everyone to have a digital identification tied to their ISP.

The principles of "know your customer" (KYC) will be imposed on everybody for everything, and anything that doesn't have that will be made illegal under National Security justifications.

Essentially, what we're looking at is a cyber Patriot Act, which will allow for the unfettered surveillance of everyone's online activities, and the ability to restrict or block access to the internet. As noted by Webb, "The internet as you know it will not exist after this happens."

The goal is to surveil all online activity in real time and have AI perform predictive policing to prevent crime before it happens. At that point, all bets are off. Data points alone may land you behind bars. Thought-crimes will also have ramifications, potentially resulting in the seizure of private property and/or removal of "privileges" previously understood as human rights.

## A Global Infrastructure Has Been Built

During their first meeting with Snowden in Hong Kong, he explained that a global infrastructure, built by the NSA with the cooperation of other governments, was already in place. That was 10 years ago, so you can imagine how it's grown since then.

At that time, that network was already automatically intercepting every digital communication, every radio communication and every analog communication. This blanket siphoning of data allows the NSA and others that have access to the network to retroactively search an individual's communications, even if all they have is a single identifier. Snowden explained:

> *"So for example, if I wanted to see the content of your email ... all I have to do is use what's called a selector, any kind of thing in the communications chain that might uniquely or almost uniquely identify you as an individual.*
>
> *I'm talking about things like email addresses, IP addresses, phone numbers, credit cards, even passwords that are unique to you that aren't used by anyone else.*

> *I can input those into the system, and it will not only go back through the database ... it will basically put an additional level of scrutiny on it moving into the future that says, 'If this is detected now or at any time in the future, I want this to go to me immediately,' and [it will] alert me in real time that you're communicating with someone. Things like that."*

According to Snowden, the British Government Communications Headquarters (GCHQ) has "the most invasive network intercept program anywhere in the world." That program, Tempora, intercepts all content, in addition to metadata, on everything and everyone.

Snowden also describes the "SSO," which stands for Special Sorters Operations. The SSO passively collects data across networks, both in the U.S. and internationally. Domestically, this is done primarily through corporate partnerships.

"They also do this with multinationals that might be headquartered in the U.S. whom [they can] just pay into giving them access," Snowden said. They also do it bilaterally with the assistance of other governments.

## You're Being Spied Upon Everywhere

Snowden also pointed out some of the many ways in which you're being spied upon by the digital devices around you. As just one example, all VoIP phones, which transmit calls over an IP network such as the internet, have little computers inside of them that can be hot mic'd even if servers are down. As long as the phone is plugged in, someone can use it to listen in on your conversations.

Within days of their first meeting in Hong Kong, Greenwald and Poitras were publishing stories about the NSA's illegal blanket spying domestically and internationally. CNN Live reported:

> *"Another explosive article has just appeared, this time in the Washington Post ... that reveals another broad and secret U.S. government's surveillance program.*

> *The Washington Post and The Guardian in London reporting that the NSA and the FBI are tapping directly into the central servers of nine leading internet companies, including Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube, and Apple.*
>
> *The Post says they're extracting audio, video, photographs, emails, documents, and connection logs that enable analysts to track a person's movements and contacts over time."*

Greenwald also made numerous live news appearances. In one, he stated:

> *"In 2008, they eliminated the warrant requirement for all conversations, except ones that take place among Americans exclusively on American soil.*
>
> *So they don't need warrants now for people who are foreigners outside of the U.S., but they also don't need warrants for Americans who are in the United States, communicating with people reasonably believed to be outside of the U.S.*
>
> *So ... the fact that there are no checks, no oversight about who's looking over the NSA's shoulder, means that they can take whatever they want, and the fact that it's all behind a wall of secrecy, and they threaten people who want to expose it, means that whatever they're doing, even violating the law is something that we're unlikely to know until we start having real investigations and real transparency into what it is that the government is doing."*

## Beyond Transparency

At this point, we're beyond merely needing transparency. The intent to surveil and control every move we make and thought we express is now being openly expressed.

We can just assume that any digital devices can and probably are collecting data on our activities and whereabouts, and that those data are nowhere near held private and can be used against us in myriad ways.

> **“Everyone must now choose between freedom and enslavement, and the option to choose freedom is rapidly closing.”**

Today, a decade after Snowden broke the dam of secrecy around the global surveillance scheme, we have but one choice left, and that is to actively reject that system by changing how we live our day to day lives. Everyone must now choose between freedom and enslavement, and the option to choose freedom is rapidly closing. Putting off making that choice is itself a choice.

Rejecting the control system means reverting back to "dumb" appliances and devices to the extent you're able. It means getting savvier about privacy technologies such as deGoogled phones and computers[2] that cannot spy on you. It means using cash as much as possible and rejecting CBDCs and digital tokens. As noted by Whitney Webb in the interview I linked to earlier:

> *"There's a huge need for to divest from Big Tech as much as possible, and it needs to happen quickly, because the choice is either participate in the system being designed for you by crazy people and become a slave, or don't become a slave. And if you don't want to be a slave, you have to invest now in Big Tech alternatives, unless you want to live a completely analog life ...*
>
> *The easiest route is to go the slavery route, and that's how they've designed it on purpose. The whole selling point of that system is that it's convenient and easy. So, obviously, it's going to take some work to go the other route, but the future of human freedom depends on it so I think it's a pretty easy choice."*

## Sources and References

- [1] PBS, My Country, My Country
- [2] Above Phone