JOHN WHITEHEAD'S COMMENTARY

Digital Trails: How the FBI Is Identifying, Tracking and Rounding Up Dissidents

By John W. Whitehead & Nisha Whitehead
March 16, 2021

> "Americans deserve the freedom to choose a life without surveillance and the government regulation that would make that possible. While we continue to believe the sentiment, we fear it may soon be obsolete or irrelevant. We deserve that freedom, but the window to achieve it narrows a little more each day. If we don't act now, with great urgency, it may very well close for good."—Charlie Warzel and Stuart A. Thompson, *New York Times*

Databit by databit, we are building our own electronic concentration camps.

With every new smart piece of smart technology we acquire, every new app we download, every new photo or post we share online, we are making it that much easier for the government and its corporate partners to identify, track and eventually round us up.

Saint or sinner, it doesn't matter because we're all being swept up into a massive digital data dragnet that does not distinguish between those who are innocent of wrongdoing, suspects, or criminals.

This is what it means to live in a suspect society.

The government's efforts to round up those who took part in the Capitol riots shows exactly how vulnerable we *all* are to the menace of a surveillance state that aspires to a God-like awareness of our lives.

Relying on selfies, social media posts, location data, geotagged photos, facial recognition, surveillance cameras and crowdsourcing, government agents are compiling a massive data trove on anyone and everyone who may have been anywhere in the vicinity of the Capitol on January 6, 2021.

The amount of digital information is staggering: 15,000 hours of surveillance and body-worn camera footage; 1,600 electronic devices; 270,000 digital media tips; at least 140,000 photos and videos; and about 100,000 location pings for thousands of smartphones.

And that's just what we know.

More than 300 individuals from 40 states have already been charged and another 280 arrested in connection with the events of January 6. As many as 500 others are still being hunted by government agents.

Also included in this data roundup are individuals who may have had nothing to do with the riots but whose cell phone location data identified them as being in the wrong place at the wrong time.

Forget about being innocent until proven guilty.

In a suspect society such as ours, the burden of proof has been flipped: now, you start off guilty and have to prove your innocence.

For instance, you didn't even have to be involved in the Capitol riots to qualify for a visit from the FBI: investigators have reportedly been tracking—and questioning—anyone whose cell phones connected to wi-fi or pinged cell phone towers near the Capitol. One man, who had gone out for a walk with his daughters only to end up stranded near the Capitol crowds, actually had FBI agents show up at his door days later. Using Google Maps, agents were able to pin-point exactly where they were standing and for how long.

All of the many creepy, calculating, invasive investigative and surveillance tools the government has acquired over the years are on full display right now in the FBI's ongoing efforts to bring the rioters to "justice."

FBI agents are matching photos with drivers' license pictures; tracking movements by way of license plate toll readers; and zooming in on physical identifying marks such as moles, scars and tattoos, as well as brands, logos and symbols on clothing and backpacks. They're poring over hours of security and body camera footage; scouring social media posts; triangulating data from cellphone towers and WiFi signals; layering facial recognition software on top of that; and then cross-referencing footage with public social media posts.

It's not just the FBI on the hunt, however.

They've enlisted the help of volunteer posses of private citizens, such as Deep State Dogs, to collaborate on the grunt work. As Dinah Voyles Pulver reports, once Deep State Dogs locates a person and confirms their identity, they put a package together with the person's name, address, phone number and several images and send it to the FBI.

According to *USA Today,* the FBI is relying on the American public and volunteer cybersleuths to help bolster its cases.

This takes See Something, Say Something snitching programs to a whole new level.

The lesson to be learned: Big Brother, Big Sister and all of their friends are watching you.

They see your every move: what you read, how much you spend, where you go, with whom you interact, when you wake up in the morning, what you're watching on television and reading on the internet.

Every move you make is being monitored, mined for data, crunched, and tabulated in order to form a picture of who you are, what makes you tick, and how best to control you when and if it becomes necessary to bring you in line.

Simply liking or sharing this article on Facebook, retweeting it on Twitter, or merely reading it or any other articles related to government wrongdoing, surveillance, police misconduct or civil liberties might be enough to get you categorized as a particular kind of person with particular kinds of interests that reflect a particular kind of mindset that *might* just lead you to engage in a particular kinds of activities and, therefore, puts you in the crosshairs of a government investigation as a potential troublemaker a.k.a. domestic extremist.

Chances are, as the *Washington Post* reports, you have already been assigned a color-coded threat score—green, yellow or red—so police are forewarned about your potential inclination to be a troublemaker depending on whether you've had a career in the military, posted a comment perceived as threatening on Facebook, suffer from a particular medical condition, or know someone who knows someone who might have committed a crime.

In other words, you might already be flagged as potentially anti-government in a government database somewhere—Main Core, for example—that identifies and tracks individuals who aren't inclined to march in lockstep to the police state's dictates.

The government has the know-how.

It took days, if not hours or minutes, for the FBI to begin the process of identifying, tracking and rounding up those suspected of being part of the Capitol riots.

Imagine how quickly government agents could target and round up any segment of society they wanted to based on the digital trails and digital footprints we leave behind.

Of course, the government has been hard at work for years acquiring these totalitarian powers.

Long before the January 6 riots, the FBI was busily amassing the surveillance tools necessary to monitor social media posts, track and identify individuals using cell phone signals and facial recognition technology, and round up "suspects" who may be of interest to the government for one reason or another.

As *The Intercept* reported, the FBI, CIA, NSA and other government agencies have increasingly invested in corporate surveillance technologies that can mine constitutionally protected speech on social media platforms such as Facebook, Twitter and Instagram in order to identify potential extremists and predict who might engage in future acts of anti-government behavior.

All it needs is the data, which more than 90% of young adults and 65% of American adults are happy to provide.

When the government sees all and knows all and has an abundance of laws to render even the most seemingly upstanding citizen a criminal and lawbreaker, then the old adage that you've got nothing to worry about if you've got nothing to hide no longer applies.

As for the Fourth Amendment and its prohibitions on warrantless searches and invasions of privacy without probable cause, those safeguards have been rendered all but useless by legislative end-runs, judicial justifications, and corporate collusions.

We now find ourselves in the unenviable position of being monitored, managed and controlled by our technology, which answers not to us but to our government and corporate rulers.

Consider that on any given day, the average American going about his daily business will be monitored, surveilled, spied on and tracked in more than 20 different ways, by both government and corporate eyes and ears. A byproduct of this new age in which we live, whether you're walking through a store, driving your car, checking email, or talking to

friends and family on the phone, you can be sure that some government agency, whether the NSA or some other entity, is listening in and tracking your behavior.

This doesn't even begin to touch on the corporate trackers that monitor your purchases, web browsing, social media posts and other activities taking place in the cyber sphere.

For example, police have been using Stingray devices mounted on their cruisers to intercept cell phone calls and text messages without court-issued search warrants. Doppler radar devices, which can detect human breathing and movement within a home, are already being employed by the police to deliver arrest warrants.

License plate readers, yet another law enforcement spying device made possible through funding by the Department of Homeland Security, can record up to 1800 license plates *per minute*. Moreover, these surveillance cameras can also photograph those *inside* a moving car. Reports indicate that the Drug Enforcement Administration has been using the cameras in conjunction with facial recognition software to build a "vehicle surveillance database" of the nation's cars, drivers and passengers.

Sidewalk and "public space" cameras, sold to gullible communities as a sure-fire means of fighting crime, is yet another DHS program that is blanketing small and large towns alike with government-funded and *monitored* surveillance cameras. It's all part of a public-private partnership that gives government officials access to all manner of surveillance cameras, on sidewalks, on buildings, on buses, even those installed on private property.

Couple these surveillance cameras with facial recognition and behavior-sensing technology and you have the makings of "pre-crime" cameras, which scan your mannerisms, compare you to pre-set parameters for "normal" behavior, and alert the police if you trigger any computerized alarms as being "suspicious."

State and federal law enforcement agencies are pushing to expand their biometric and DNA databases by requiring that anyone accused of a misdemeanor have their DNA collected and catalogued. However, technology is already available that allows the government to collect biometrics such as fingerprints from a distance, without a person's cooperation or knowledge. One system can actually scan and identify a fingerprint from nearly 20 feet away.

Developers are hard at work on a radar gun that can actually show if you or someone in your car is texting. Another technology being developed, dubbed a "textalyzer" device, would allow police to determine whether someone was driving while distracted. Refusing to submit one's phone to testing could result in a suspended or revoked driver's license.

It's a sure bet that anything the government welcomes (and funds) too enthusiastically is bound to be a Trojan horse full of nasty, invasive surprises.

Case in point: police body cameras. Hailed as the easy fix solution to police abuses, these body cameras—made possible by funding from the Department of Justice—turn police officers into roving surveillance cameras. Of course, if you try to request access to that footage, you'll find yourself being led a merry and costly chase through miles of red tape, bureaucratic footmen and unhelpful courts.

The "internet of things" refers to the growing number of "smart" appliances and electronic devices now connected to the internet and capable of interacting with each other and being controlled remotely. These range from thermostats and coffee makers to cars and TVs. Of course, there's a price to pay for such easy control and access. That price amounts to relinquishing ultimate control of and access to your home to the government and its corporate partners. For example, while Samsung's Smart TVs are capable of "listening" to what you say, thereby allowing users to control the TV using voice commands, it also records everything you say and relays it to a third party, e.g., the government.

Then again, the government doesn't really need to spy on you using your smart TV when the FBI can remotely activate the microphone on your cellphone and record your conversations. The FBI can also do the same thing to laptop computers without the owner knowing any better.

Drones, which are taking to the skies en masse, are the converging point for all of the weapons and technology already available to law enforcement agencies. In fact, drones can listen in on your phone calls, see through the walls of your home, scan your biometrics, photograph you and track your movements, and even corral you with sophisticated weaponry.

All of these technologies add up to a society in which there's little room for indiscretions, imperfections, or acts of independence, especially not when the government can listen in on your phone calls, monitor your driving habits, track your movements, scrutinize your purchases and peer through the walls of your home.

These digital trails are everywhere.

As investigative journalists Charlie Warzel and Stuart A. Thompson explain, "This data—collected by smartphone apps and then fed into a dizzyingly complex digital advertising ecosystem … provided an intimate record of people whether they were visiting drug treatment centers, strip clubs, casinos, abortion clinics or places of worship."

In such a surveillance ecosystem, we're all suspects and databits to be tracked, catalogued and targeted.

As Warzel and Thompson warn:

> "To think that the information will be used against individuals only if they've broken the law is naïve; such data is collected and remains vulnerable to use and abuse whether people gather in support of an insurrection or they justly protest police violence… This collection will only grow more sophisticated… It gets easier by the day… it does not discriminate. It harvests from the phones of MAGA rioters, police officers, lawmakers and passers-by. There is no evidence, from the past or current day, that the power this data collection offers will be used only to good ends. There is no evidence that if we allow it to continue to happen, the country will be safer or fairer."

As I point out in my book *Battlefield America: The War on the American People*, this is the creepy, calculating yet diabolical genius of the American police state: the very technology we hailed as revolutionary and liberating has become our prison, jailer, probation officer, Big Brother and Father Knows Best all rolled into one.

There is no gray area any longer.

WC: 2388

ABOUT JOHN W. WHITEHEAD

Constitutional attorney and author John W. Whitehead is founder and president The Rutherford Institute. His books *Battlefield America: The War on the American People* and *A Government of Wolves: The Emerging American Police State* are available at www.amazon.com. He can be contacted at johnw@rutherford.org. Nisha Whitehead is the Executive Director of The Rutherford Institute. Information about The Rutherford Institute is available at www.rutherford.org.

Publication Guidelines / Reprint Permission