We the Targeted: How the Government Weaponizes Surveillance to Silence Its Critics

<u>We the Targeted: How the Government Weaponizes</u> <u>Surveillance to Silence Its Critics</u>

by <u>John & Nisha Whitehead</u>, <u>The Rutherford Institute</u> August 29, 2023

"Once a government is committed to the principle of silencing the voice of opposition, it has only one way to go, and that is down the path of increasingly repressive measures, until it becomes a source of terror to all its citizens and creates a country where everyone lives in fear."

President Harry S. Truman

Ever since Martin Luther King Jr. delivered his groundbreaking "I Have a Dream" speech during the March on Washington for Jobs and Freedom on Aug. 28, 1963, the Deep State has been hard at work turning King's dream into a living nightmare.

The end result of the government's efforts over the past 60 years is a country where nothing ever really changes, and everyone lives in fear.

Race wars are still being stoked by both the Right and the Left; the military-industrial complex is still waging profitdriven wars at taxpayer expense; the oligarchy is still calling the shots in the seats of government power; and the government is still weaponizing surveillance in order to

muzzle anti-government sentiment, harass activists, and terrorize Americans into compliance.

This last point is particularly disturbing.

Starting in the 1950s, the government relied on COINTELPRO, its domestic intelligence program, to neutralize domestic political dissidents. Those targeted by the FBI under COINTELPRO for its intimidation, surveillance and smear campaigns included: Martin Luther King Jr., Malcom X, the Black Panther Party, John Lennon, Billie Holiday, Emma Goldman, Aretha Franklin, Charlie Chaplin, Ernest Hemingway, Felix Frankfurter, and hundreds more.

In more recent decades, the powers-that-be have expanded their reach to target anyone who opposes the police state, regardless of their political leanings.

Advances in technology have enabled the government to deploy a veritable arsenal of surveillance weapons in order to "expose, disrupt, misdirect, discredit, or otherwise neutralize" perceived threats to the government's power.

Surveillance cameras mounted on utility poles, traffic lights, businesses, and homes. License plate readers. Ring doorbells. GPS devices. Dash cameras. Drones. Store security cameras. Geofencing and geotracking. FitBits. Alexa. Internet-connected devices. Geofencing dragnets. Fusion centers. Smart devices. Behavioral threat assessments. Terror watch lists. Facial recognition. Snitch tip lines. Biometric scanners. Pre-crime. DNA databases. Data mining. Precognitive technology. Contact tracing apps.

What these add up to is a world in which, on any given day, the average person is now monitored, surveilled, spied on and tracked in more than 20 different ways by both government and corporate eyes and ears.

Consider just a small sampling of the ways in which the

government is weaponizing its 360 degree surveillance technologies to flag you as a threat to national security, whether or not you've done anything wrong.

Flagging you as a danger based on your feelings. Customs and Border Protection is reportedly using an artificial intelligence surveillance program that can detect "sentiment and emotion" in social media posts in order to identify travelers who may be "a threat to public safety, national security, or lawful trade and travel."

Flagging you as a danger based on your phone and movements. Cell phones have become de facto snitches, offering up a steady stream of digital location data on users' movements and travels. For instance, the FBI was able to use geofence data to identify more than 5,000 mobile devices (and their owners) in a 4-acre area around the Capitol on January 6. This latest surveillance tactic could land you in jail for being in the "wrong place and time." Police are also using cell-site simulators to carry out mass surveillance of protests without the need for a warrant. Moreover, federal agents can now employ a number of hacking methods in order to gain access to your computer activities and "see" whatever you're seeing on your monitor. Malicious hacking software can also be used to remotely activate cameras and microphones, offering another means of glimpsing into the personal business of a target.

Flagging you as a danger based on your DNA. DNA technology in the hands of government officials completes our transition to a Surveillance State. If you have the misfortune to leave your DNA traces anywhere a crime has been committed, you've already got a file somewhere in some state or federal database—albeit it may be a file without a name. By accessing your DNA, the government will soon know everything else about you that they don't already know: your family chart, your ancestry, what you look like, your health history, your inclination to follow orders or chart your own course, etc. After all, a DNA print reveals everything about "who we are, where we come

from, and who we will be." It can also be used to predict the physical appearance of potential suspects. It's only a matter of time before the police state's pursuit of criminals expands into genetic profiling and a preemptive hunt for criminals of the future.

Flagging you as a danger based on your face. Facial recognition software aims to create a society in which every individual who steps out into public is tracked and recorded as they go about their daily business. Coupled with surveillance cameras that blanket the country, facial recognition technology allows the government and its corporate partners to identify and track someone's movements in realtime. One particularly controversial software program created by Clearview AI has been <u>used</u> by <u>police</u>, the <u>FBI</u> and the <u>Department of Homeland Security to collect photos on social</u> media sites for inclusion in a massive facial recognition database. Similarly, biometric software, which relies on one's unique identifiers (fingerprints, irises, voice prints), is becoming the standard for navigating security lines, as well as bypassing digital locks and gaining access to phones, computers, office buildings, etc. In fact, greater numbers of travelers are opting into programs that rely on their biometrics in order to avoid long waits at airport security. Scientists are also developing lasers that can <u>identify</u> and surveil individuals based on their heartbeats, scent and microbiome.

Flagging you as a danger based on your behavior. Rapid advances in behavioral surveillance are not only making it possible for individuals to be monitored and tracked based on their patterns of movement or behavior, including gait recognition (the way one walks), but have given rise to whole industries that revolve around predicting one's behavior based on data and surveillance patterns and are also shaping the behaviors of whole populations. One smart "antiriot" surveillance system purports to predict mass riots and

<u>unauthorized public events</u> by using artificial intelligence to analyze social media, news sources, surveillance video feeds and public transportation data.

Flagging you as a danger based on your spending and consumer activities. With every smartphone we buy, every GPS device we install, every Twitter, Facebook, and Google account we open, every frequent buyer card we use for purchases—whether at the grocer's, the yogurt shop, the airlines or the department store—and every credit and debit card we use to pay for our transactions, we're helping Corporate America build a dossier for its government counterparts on who we know, what we think, how we spend our money, and how we spend our time. Consumer surveillance, by which your activities and data in the physical and online realms are tracked and shared with advertisers, has become a \$300 billion industry that routinely harvests your data for profit. Corporations such as Target have not only been tracking and assessing the behavior of their customers, particularly their purchasing patterns, for years, but the retailer has also funded major surveillance in the country and developed cities across behavioral surveillance algorithms that can determine whether someone's mannerisms might fit the profile of a thief.

Flagging you as a danger based on your public activities. Private corporations in conjunction with police agencies throughout the country have created a web of surveillance that encompasses all major cities in order to monitor large groups of people seamlessly, as in the case of protests and rallies. They are also engaging in extensive online surveillance, looking for any hints of "large public events, social unrest, gang communications, and criminally predicated individuals." Defense contractors have been at the forefront of this lucrative market. Fusion centers, \$330 million-a-year, information-sharing hubs for federal, state and law enforcement agencies, monitor and report such "suspicious" behavior as people buying pallets of bottled water,

photographing government buildings, and applying for a pilot's license as "suspicious activity."

Flagging you as a danger based on your social media activities. Every move you make, especially on social media, is 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. As The Intercept reported, the FBI, CIA, NSA and other government agencies are increasingly investing in and relying on 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. This obsession with social media as a form of surveillance will have some <u>frightening</u> consequences in coming years. As Helen A.S. Popkin, writing for NBC News, observed, "We may very well face a future where algorithms bust people en masse for referencing illegal 'Game of Thrones' downloads... the new software has the potential to roll, Terminator-style, targeting every social media user with a shameful confession or questionable sense of humor."

Flagging you as a danger based on your social network. Not content to merely spy on individuals through their online activity, government agencies are now using <u>surveillance</u> technology to track one's social network, the people you might connect with by phone, text message, email or through social message, in order to ferret out possible criminals. An FBI document obtained by Rolling Stone speaks to the ease with which agents are <u>able to access address book data from Facebook's WhatsApp and Apple's iMessage services</u> from the accounts of targeted individuals and individuals not under investigation who might have a targeted individual within their network. What this creates is a "guilt by association" society in which we are all as guilty as the most culpable

person in our address book.

Flagging you as a danger based on your car. License plate readers are mass surveillance tools that can photograph over 1,800 license tag numbers per minute, take a picture of every passing license tag number and store the tag number and the date, time, and location of the picture in a searchable database, then share the data with law enforcement, fusion centers and private companies to track the movements of persons in their cars. With tens of thousands of these license plate readers now in operation throughout the country, affixed to overpasses, cop cars and throughout business sectors and residential neighborhoods, it allows police to track vehicles and run the plates through law enforcement databases for abducted children, stolen cars, missing people and wanted fugitives. Of course, the technology is not infallible: there have been numerous incidents in which police have mistakenly relied on license plate data to capture out suspects only to end up detaining innocent people at gunpoint.

Flagging you as a danger based on your political views. The Church Committee, the Senate task force charged with investigating COINTELPRO abuses in 1975, concluded that the government had carried out "secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power." The report continued: "Groups and individuals have been harassed and disrupted because of their political views and their lifestyles... Intelligence agencies have served the political and personal objectives of presidents and other high officials." Nothing has changed since then.

Flagging you as a danger based on your correspondence. Just about every branch of the government—from the Postal Service to the Treasury Department and every agency in between—now has its own surveillance sector, authorized to spy on the American people. For instance, the U.S. Postal Service, which has

been photographing the exterior of every piece of paper mail for the past 20 years, is also spying on Americans' texts, emails and social media posts. Headed up by the Postal Service's law enforcement division, the Internet Covert Operations Program (iCOP) is reportedly using facial recognition technology, combined with fake online identities, to ferret out potential troublemakers with "inflammatory" posts. The agency claims the online surveillance, which falls outside its conventional job scope of processing and delivering paper mail, is necessary to help postal workers avoid "potentially volatile situations."

Now the government wants us to believe that we have nothing to fear from these mass spying programs as long as we've done nothing wrong.

Don't believe it.

As Matthew Feeney warns in the *New York Times*, "In the past, Communists, civil rights leaders, feminists, Quakers, folk singers, war protesters and others have been on the receiving end of law enforcement surveillance. No one knows who the next target will be."

The government's definition of a "bad" guy is extraordinarily broad, and it results in the warrantless surveillance of innocent, law-abiding Americans on a staggering scale.

Moreover, there is a repressive, suppressive effect to surveillance that not only acts as a potentially small deterrent on crime but serves to monitor and chill lawful First Amendment activity, and that is the whole point.

Weaponized surveillance is re-engineering a society structured around the aesthetic of fear.

As I make clear in my book <u>Battlefield America: The War on the American People</u> and in its fictional counterpart <u>The Erik Blair Diaries</u>, the police state wants us silent, servile and

compliant.

They definitely do not want us to engage in First Amendment activities that challenge the government's power, reveal the government's corruption, expose the government's lies, and encourage the citizenry to push back against the government's many injustices.

And they certainly do not want us to remember that we have rights, let alone attempting to exercise those rights peaceably and lawfully, whether it's protesting police brutality and racism, challenging COVID-19 mandates, questioning election outcomes, or listening to alternate viewpoints—even conspiratorial ones—in order to form our own opinions about the true nature of government.

Connect with The Rutherford Institute

Cover image credit: <u>Tumisu</u>