



# You'd Better Watch Out: The Surveillance State Is Making a List, and You're on It

*“He sees you when you're sleeping  
He knows when you're awake  
He knows when you've been bad or  
good  
So be good for goodness' sake!”  
—“Santa Claus Is Coming to Town”*



John Whitehead

You'd better watch out—you'd better not pout—you'd better not cry—'cos I'm telling you why: this Christmas, it's the Surveillance State that's making a list and checking it twice, and it won't matter whether you've been bad or good.

You'll be on *this* list whether you like it or not.

Mass surveillance is the Deep State's version of a “gift” that keeps on giving...back to the Deep State.

[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.

Big Tech wedded to Big Government has become Big Brother.

Every second of every day, the American people are being spied on by a vast network of digital Peeping Toms, electronic eavesdroppers and robotic snoops.

This creepy new era of government/corporate spying—in which we're being listened to, watched, tracked, followed, mapped, bought, sold and targeted—has been made possible by a global army of techno-tyrants, fusion centers and Peeping Toms.

Consider just a small sampling of the tools being used to track your movements, monitor your spending, and sniff out all the ways in which your thoughts, actions and social circles might land you on the government's naughty list, whether or not you've done anything wrong.

**Tracking you 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 four-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



Written by [John and Nisha Whitehead](#) on December 14, 2022

---

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.

**Tracking you 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](#).

**Tracking you 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 real time. One particularly controversial software program created by Clearview AI has been [used by police, the FBI and the Department of Homeland Security to collect photos on social 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 [identify and surveil individuals based on their heartbeats, scent and microbiome](#).

**Tracking you 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 “anti-riot” surveillance system purports to [predict mass riots and unauthorized public events](#) by using artificial intelligence to analyze social media, news sources, surveillance video feeds and public transportation data.

**Tracking you 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 big business, 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 cities across the country and developed behavioral surveillance [algorithms that can determine whether someone’s](#)



Written by [John and Nisha Whitehead](#) on December 14, 2022

---

[mannerisms might fit the profile of a thief.](#)

**Tracking you 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 local 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.”

**Tracking you 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 [frightening 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.”

**Tracking you based on your social network:** Not content to merely spy on individuals through their online activity, government agencies are now using [surveillance 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 [able to access address book data from Facebook’s WhatsApp and Apple’s iMessage services](#) 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.

**Tracking you 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. 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, allow 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 suspects only to end up detaining innocent people at gunpoint.

**Tracking you based on your mail:** 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



Written by [John and Nisha Whitehead](#) on December 14, 2022

---

[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.

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.

As I make clear in my book [Battlefield America: The War on the American People](#) and in its fictional counterpart [The Erik Blair Diaries](#), surveillance, digital stalking and the data mining of the American people—weapons of compliance and control in the government's hands—haven't made America any safer. And they certainly aren't helping to preserve our freedoms.

Indeed, America will never be safe as long as the U.S. government is allowed to shred the Constitution.

#### ABOUT JOHN & NISHA WHITEHEAD:

*Constitutional attorney and author John W. Whitehead is founder and president of The Rutherford Institute. His latest books [The Erik Blair Diaries](#) and [Battlefield America: The War on the American People](#) are available at [www.amazon.com](http://www.amazon.com). Whitehead can be contacted at [johnw@rutherford.org](mailto:johnw@rutherford.org). Nisha Whitehead is the Executive Director of The Rutherford Institute. Information about The Rutherford Institute is available at [www.rutherford.org](http://www.rutherford.org).*



## Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



[Subscribe](#)

### What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.