You’d Better Watch Out: The Surveillance State Has a Naughty List, and You’re On It

You’d Better Watch Out: The Surveillance State Has a Naughty List, and You’re On It

by **John W. Whitehead & Nisha Whitehead**, *The Rutherford Institute*
December 7, 2021

> *“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”*

Santa’s got a new helper.

No longer does the all-knowing, all-seeing, jolly Old St. Nick need to rely on antiquated elves on shelves and other seasonal snitches in order to know when you’re sleeping or awake, and if you’ve been naughty or nice.

Thanks to the government’s almost limitless powers made possible by a domestic army of techno-tyrants, fusion centers and Peeping Toms, Santa can get real-time reports on who’s been good or bad this year. This creepy new era of government/corporate spying—in which we’re being listened to,

watched, tracked, followed, mapped, bought, sold and targeted—makes the NSA's rudimentary phone and metadata surveillance appear almost antiquated in comparison.

Consider just a small sampling of the tools being used to track our movements, monitor our spending, and sniff out all the ways in which our thoughts, actions and social circles might land us on the government's naughty list.

Tracking you based on your health status. In the age of COVID-19, digital health passports are gaining traction as gatekeepers of a sort, restricting access to travel, entertainment, etc., based on one's vaccine status. Whether or not one has a vaccine passport, however, individuals may still have to prove themselves "healthy" enough to be part of society. For instance, in the wake of Supreme Court rulings that paved the way for police to use drug-sniffing dogs as "search warrants on leashes," government agencies are preparing to use virus-detecting canine squads to carry out mass screenings to detect individuals who may have COVID-19. Researchers claim the COVID-sniffing dogs have a 95% success rate of identifying individuals with the virus (except when they're hungry, tired or distracted). These dogs are also being to trained to ferret out individuals suffering from other health ailments such as cancer.

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 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 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 phone and online activities: Cell phones have become de facto snitches, offering up a steady stream of digital location data on users’ movements and travels. Police have used 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.

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.

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.

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 *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."

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.

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—add up to a society in which there's little room for indiscretions, imperfections, or acts of independence.

In an age of overcriminalization, mass surveillance, and an appalling lack of protections for our privacy rights, we can all be considered guilty of some transgression or other.

So 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 coming to town, and you're already on its naughty list.

Connect with The Rutherford Institute

cover image credit: biggerthanpluto / pixabay