BIG BROTHER'S WATCHING

HOW MUCH DOES HE KNOW AND WHAT YOU CAN DO ABOUT IT?

JACK CRIVALLE

Big Brother is Watching: What Does He Know About You?
Published by Suburban Graphics Press
Oak Lawn, Illinois

DISCLAIMER
Names, characters, businesses, places, events, locales, and incidents are either the products of the author's imagination or used in a fictitious manner. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Publisher's Cataloging-in-Publication Data

Names: Crivalle, Jack, author. Title: Big Brother is watching / by: Jack Crivalle. Description: Oak Lawn, Illinois : Suburban Graphics Publishing, [2024] | Includes bibliographical references. Identifiers: Subjects: Classification: ISBN: 979-8-9872158-7-6 (paperback) | 979-8-9872158-6-9 (hardcover) LCSH: Electronic surveillance--Social aspects. | Video surveillance--Social aspects. | Internet --Social aspects. | Intelligence service--Social aspects. | Drone aircraft--Social aspects. | Technology--Social aspects. | Social control--Technological innovations. | Vigilance (Psychology) | Privacy, Right of. | Computer security. | Space surveillance. | Public records-- Access control. | Technology and state. | BISAC: TRUE CRIME / Cybercrime. LCC: HM853 .C75 2024 | DDC: 363.2/32—dc

Cover and interior design by Victoria Wolf, wolfdesignandmarketing.com, Copy line Editor, Sheila Maloney and Proof editor, copyright owned by Jack Crivalle.

I would like to dedicate this book to my family, my wife Cathy, my sons, Thomas, Andrew, and Alex, all of whom I love dearly.

I would also like to thank my dear brother-in-law Mike Cavanaugh, who always encouraged me to write and was always overjoyed with my accomplishments.

CONTENTS

Introduction vii

CHAPTER 1 Surveillance Cameras 1

CHAPTER 2 Cell Phone a Necessity and a Nightmare 13

CHAPTER 3 How Our Computers Track Us ... 25

CHAPTER 4 How the Tollway System Spies on Us 33

CHAPTER 5 Satellite Spying 39

CHAPTER 6 Spy Drones 43

CHAPTER 7 Spy Planes 51

CHAPTER 8 The USA Patriot Act 57

CHAPTER 9 Your Neighbor, Your Co-Worker, and Your Friend..... 69

CHAPTER 10 Beware of the Utility Companies 77

CHAPTER 11 Credit Card and Debit Card Intrusion 85

CHAPTER 12 Spying on Our Vacations 93

CHAPTER 13 How the Government
Uses Our DNA Against Us.....97

CHAPTER 14 Fingerprinting Fulfillment .109

CHAPTER 15 Biometric Data 115

CHAPTER 16 Your Physician,
Your Pharmacy, and Your Health Club....125

CHAPTER 17 Fight Back: Deflecting
Big Brother 131

Epilogue 139

Endnotes 151

Acknowledgments 157

About the Author 159

INTRODUCTION

THE PEOPLE OF THE UNITED STATES are slowly becoming enslaved. These are strong words, scary words, and words that can, if focused on, help change the narrative of what we, as a temporary free society, are heading for.

Recently, I read both the book *1984* and watched the 1956 movie by the same name. It portrays a world filled with a multitude of cameras and spy equipment. This technology is focused on the general population to keep them subservient and obedient. There is no privacy. The country, government, and the party rule all and know everyone's every movement. This isn't far off our mark. Both communism and fascism accomplished this with complete success in the early part of the twentieth century. These governments had an extensive spy network with informants, phone taps, and surveillance on every sector of their society. There was no such thing as freedom, and merely saying the word could land you in custody with severe repercussions. Today North Korea is so twisted that their population has very little knowledge of the outside world. A small segment of the North Korea population controls the rest of the country. The Kim Dynasty

has ruled over North Korea for over seven decades. Through repression, intimidation, and purges, one family controls the rest of the population of around twenty-five million.

Moreover, all governments around the world have a multitude of surveillance measures to protect their populations from "terrorism," so they say. In all honesty, these measures do help protect honest citizens from terrorist evils. However, does it do more to stifle our freedoms? This will be explored in depth and hopefully, help open the eyes of us average men and women before it's too late to do anything about it.

After reading and watching *1984,* I was frightened. The reason being is that I started paying more attention to my surroundings during my daily activities. The day after reading and watching *1984,* I woke up early as usual. I showered, and then I logged onto my computer to read and write emails. This social habit is trackable. Everything that we do or say on these emails and websites can be tracked and, in many cases, is. I even received an email from my credit union saying that a scan was done of my data, a routine measure that they do for security purposes, and some of my data was discovered on the dark web. In case you are unfamiliar with the dark web, it is a part of the Internet that allows users to hide their identity and location from others. Some even claim that these dark web operators even hide from law enforcement, which, in my opinion, is highly unlikely. It is made up of encrypted online content that is not indexed by standard search engines, such as email accounts, bank accounts, and databases. The dark web is made up of small "friend to friend" accounts as well as larger networks operated by public organizations. This dark web consists of a multitude of hacking tools and individuals who perform a variety of unethical acts, such as claiming unemployment under another person's name, applying for our tax refunds, and prying into our bank and credit card accounts.

While leaving my home, I grabbed my cell phone, which I always carry

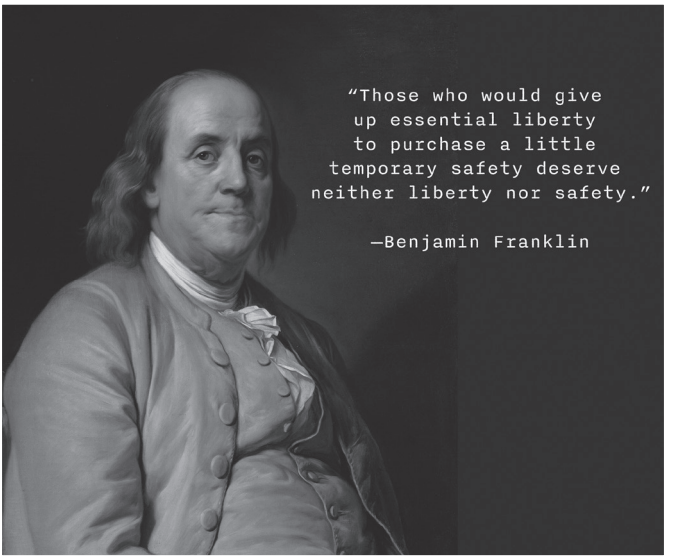
with me as just another personal item. We all joke about how attached we are to these phones that also function as a minicomputer. These are brilliant items that have revolutionized our entire society. While we are traveling, we will pass by a series of cell towers. We are all being tracked as we pass each tower, which is called trilateration/triangulation, and I will discuss this in more detail in the body of this book. Suffice it to say for now that it is a scary practice, whereby we are all tracked within yards of our actual locations via our cell phones. Also, there are other varieties of cell phone interrogation, such as, who we called that morning, what we viewed, and what we researched.

As I drove merrily down the road toward my work destination, I noticed a series of red lights and stoplight cameras along the way. Later research on these cameras revealed to me that they are *always* on. I thought that they only turn on when they are activated during an infraction, like speeding or going through a red light. However, this is not the case. So, during my twelve-mile rush hour commute, which took me forty-five minutes to complete, I was captured by five different cameras.

After arriving at my destination, I parked my car and walked two blocks to the building where I work, being picked up yet again by another surveillance camera. After entering the building, I noticed three more cameras in the lobby and one in the elevator. I was then able to make it to my desk and log onto my computer, which welcomed me as I logged in my personal codes that only recognized me.

So, there you have it—I woke up at six a.m. and I was now sitting at my desk at eight a.m. I was only awake and active for two hours, yet I was tracked over twelve times. During the remainder of my day, I estimate that I had driven or walked past another twenty-five cameras as well as several cell towers that pinged my phone. Big Brother is watching, and I have become very uncomfortable with it. Where is my privacy? What happened to it?

Benjamin Franklin stated quite poignantly, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety!"



CHAPTER 1 _

Surveillance Cameras

SURVEILLANCE CAMERAS ARE NOT NEW TECHNOLOGY. The technology dates to the 1940s when German military researchers developed the first Closed Circuit Television (CCTV) system to monitor bomber runways at night. These early systems were large and required a lot of cabling, and the security footage could only be monitored in real time.

In the late 1940s US contractors began developing and selling CCTV systems commercially. In 1953, British officials reportedly used surveillance systems for the royal coronation. The first documented use of surveillance cameras was in the Soviet Union during Stalin's reign. Evidently, Stalin knew the potential of his new spying devices and undoubtedly used it to spy on and subjugate the Soviet population.

In the twenty-first century, innovation and technology have transformed security cameras into complex systems integrated with both artificial intelligence (AI) and the Internet. In 2024, surveillance and spy cameras have become more advanced at handling challenging imaging conditions, especially harsh lighting and darkness.

For example, security cameras will record any movement through infrared technology that sets the camera's program in motion by activating an internal motion sensor generated by body heat. After recording in color during the day, the cameras automatically switch to black and white night vision for extra nighttime clarity.

Ironically, I was part owner of a security company in Chicago for ten years. We offered security guards, off-duty police officers, special investigations, and electronic security in the form of burglar alarms and surveillance cameras. At that time all of these were exclusively security measures offering protection against theft and violence.

Surveillance cameras have been proven to be a crime deterrent as well as a good witness to almost any crime. The old adage goes, "The camera doesn't lie."

However, as Benjamin Franklin asked, "Are we sacrificing freedom for temporary security?" It has always been known through government crime statistics that 90 percent of the population has to protect themselves from the other 10 percent. It is no secret that 10 percent of the population is deleterious and hard to deal with. Society tries hard to detain, incarcerate, and impede this 10 percent whenever possible, but at times, they are so bad that honest, law-abiding citizens take many extraordinary measures to protect themselves and their families.

So, we can establish that these surveillance cameras do help to protect us, but at what cost? The laws regulating surveillance vary from state to state. There are no federal laws that restrict the use of surveillance cameras. The common denominator between states, however, is that most states forbid any security cameras in private areas like washrooms, changing rooms, bedrooms, locker rooms, and hotel rooms. Private property is exempt from these laws. Anyone can utilize surveillance cameras to protect their own property without restrictions. Video recordings that also record voice and audio are prohibited without consent from all being recorded. However, there is a loophole in this. There is something called the "one-party consent law." Thirty-eight states and the District of Columbia have adopted the one-party consent law.

One-party consent laws state that one person can record a conversation without telling the other person. Under one-party consent, a person can record a conversation without the other party knowing. In Virginia, however, it is a felony to record a phone call without the consent of at least one party, or with criminal or tortious intent. In Wisconsin, it is a felony to record a phone call without the consent of at least one party. However, not all states follow the rule.

Like anything, technology can be used for both good and evil. There are a vast number of spy cameras on the market that are specifically marketed as spy cameras. They can be both disguised and hidden. Some may be hidden behind glass or a mirror, while others are hidden in smoke detectors and light switches. Anyone can buy these by just checking out the World Wide Web. Amazon carries a large assortment. So, as I discussed previously, I know of being tracked by at least twenty-five cameras in one day. However, those were the visible cameras, the ones we can easily see. How many cameras are tracking us covertly?

The future outlook of the wireless spy camera market appears to be growing, and the future business opportunities for entrepreneurs in the security industry are promising. Factors driving this growth include the rising need for surveillance in public places, the increasing adoption of smart home systems, and the advancements in technology.[1]

Ring cameras (and other brands of doorbell cameras) installed on homes have become cheaper and more prevalent. It is estimated that 20 percent of all the new cameras installed will be these ubiquitous devices. These spy cameras are often preferred over wired surveillance cameras due to their ease of installation and flexibility in placement. Moreover, they are unobtrusive, so people don't necessarily see them and do not know they are being watched, giving people a false sense of privacy.

Additionally, the increased use of wireless spy cameras in industries such as retail, hospitals, and health care facilities is further fueling the market growth. Retailers, for example, utilize these cameras to monitor customer behavior, prevent theft, and enhance overall security. At the same time, the personal lives of both the employees and customers are also observed. It is not uncommon for surveillance cameras and spy camera video footage to be subpoenaed on a regular basis as evidence in a multitude of proceedings.[2]

It is my opinion, as well as that of many freedom and privacy

advocates, that surveillance and spy cameras pose the biggest threat to privacy when used excessively or without proper regulation. These cameras can:

- **Constantly Monitor**

Cameras can constantly monitor people's activities without their consent, especially when used in public places by governments, schools, and public forums and facilities.

- **Location Track**

Modern surveillance systems equipped with modern technology include facial recognition and license plate recognition.

- **Data Collect**

Surveillance and spy cameras can gather a large amount of data about people, including their appearance, behaviors, and activities.

- **Inadvertently Capture Sensitive Information**

Cameras can capture personally identifiable details, confidential conversations, and private activities.

- **Facilitate Hackers**

Hackers can track videos or upload them to the Internet. However, there are some ways for the installer and benefactor of surveillance and spy cameras to prevent being hacked. For example, they can integrate

the built-in privacy features into the cameras. Also, disabling the audio microphones is a good idea.

Furthermore, this level of surveillance leads to bad policies that can lead to abusive ends, especially during periods of social turmoil or conflicts over government policies.

Luckily, so far, the technology for security cameras, although vast, has not conquered the problem of data storage yet. The security surveillance and spy cameras data is fed into a computer. To store imagery, it takes up a lot of storage. That imagery is placed on a storage loop in the computer database that is programmed to run off at a certain time. Some run off in as little as a couple of days, some fifteen days, and the vast majority thirty days. However, there are some bigger money organizations, like big business and the government, that can afford to pay for extra computer storage for up to a year. This is the state of data storage today. If (or when) someone makes data storage cheap or even free, we will then face an entirely new set of problems, as these videos will never be erased. Is that what we want?

And finally, no one is watching the watchers.

Nobody expects to be invisible on streets, at borders, or in shopping centers. But who has access to all the surveillance data? Surveillance and spy cameras may be used by public authorities or even individuals for their own purposes. Since video surveillance often contains images of people, this activity is considered a use of personal information and could implicate serious privacy risks. These same cameras can also put people who own them at risk. They're vulnerable to hacks, and sensitive footage can be mishandled by companies and undisciplined employees.[3]

Public surveillance, or mass surveillance, can threaten privacy and limit free expression and association. Examples are biometric mass surveillance that can collect large amounts of data without the user's knowledge, such as facial recognition and retinal scans, fingerprints, and

voice inflection imprinting. Surveillance can also be abused, such as when law enforcement uses information gathered by cameras for blackmail or when innocent victims are spied on in public.[4]

Mass surveillance is also indiscriminate surveillance. These systems use technology to collect, analyze and/or generate data on an infinite number of people instead of limiting surveillance to individuals about which there is reasonable suspicion of them committing wrongdoing. Under current available forms of mass surveillance, governments can capture virtually all aspects of our lives. This should scare every free-thinking American as well as international believers in liberty. Being spied on constantly with cameras is a violation of all that freedom and liberty is.

The science of mass surveillance subjects a population to indiscriminate monitoring, involving a systematic interference with people's right to privacy and all the rights that privacy enables us, including the freedom to express ourselves and to protest. This can easily subjugate a population to government and even corporate oppression.

Today, intelligence agencies and law enforcement conduct mass surveillance through a diverse and increasing range of means and methods of surveillance. These include the direct mass interpretation of communications, access to the bulk communications stored by telecom operators and others, mass hacking, and indiscriminate use of surveillance of protests using mobile phone hacking.

Mass surveillance involves the acquisition, processing, generation, analysis, use, retention, or storage of information about large numbers of people. This is without any regard to whether they are suspected of wrongdoing.

In legal terms, the problem with mass surveillance is that it is neither strictly necessary nor proportionate in a democratic society. There are often less invasive alternatives. And even when there may not be, we must question whether a democratic society can survive under constant

surveillance. To date, a free and democratic society has never been surveilled as it is now being surveilled in our era.

By analytically monitoring people's lives, mass surveillance enables the potential for unchecked state and corporate control over individuals. Mass surveillance relies on the assumption that all information could be used to address a hypothetical threat, which is irreconcilable with the fundamental values and principles of democratic societies that seek to limit the information a state knows about its people to moderate its power.

Mass camera surveillance also obstructs the separation of powers as the executive branch can carry out its operations without sufficient stringent oversight from two other powers—the legislative and judicial. No legal oversight is invoked in this intelligence gathering as it is being done under the guise of national intelligence and security. Mass surveillance powers lack effective independent authorization, as the ability to surveil is authorized in bulk instead of regarding each instance of wrongdoing. It creates an environment of threat and suspicion that is incompatible with democratic values and principles, where in the eyes of the state, all individuals become guilty until proven innocent.

Mass surveillance negatively affects other human rights and freedoms. Unjustified interferences with privacy prevent the enjoyment of other rights and often provide a gateway to the violation of other freedoms. Most notably, freedoms at risk include freedoms of assembly, expression, movement, and implicate principles of nondiscrimination and political participation.

Law enforcement is given an ample amount of leeway with these surveillance measures. By surveilling and reading license plates at random, they can run a citizen's plate at will to see what the person's background is. For example, if a particular citizen has been convicted of driving under the influence, then is there a probable cause to pull them over, or can they make a stop under another assumption just to follow up on the surveillance?

We're facing the end of privacy in public because of the unchecked rise of facial recognition technology in public spaces, shops, restaurants, and bars.

In the United States, we live in a representative republic where our elected leaders are supposed to be looking out for our best interests, but are they? I received a speeding ticket from a government speed camera (which is actually unconstitutional, but that is a book for a later day). The camera was so powerful that it showed a clear picture of the inside of my car. The photo showed the color of my hair, and even the thinning hair area on my scalp. If the function of this camera was to catch people speeding, then why didn't it just read my license plate?

Ironically, many businesses opt to buy cameras from the lowest bidder, which leaves them with a substandard camera with a grainy image. However, government can afford the best and often buy high-end powerful cameras that see all. It will only be getting worse as technology gets better, depending on what perspective a person interprets surveillance, security, liberty, and freedom.

We talk a lot about governmental intrusion in our private lives, but big business has become just as intrusive, if not more. I worked for a large publishing company out of St. Louis and saw firsthand how they developed a spy network and eavesdropped on their employees. They listened in on employee's phone conversations, through complete use of CCTV cameras. I worked for this company in the 1980s, so cameras were still not a big deal yet. However, as frugal a company as they were, they invested in cameras. Their fear of reprisal from the working population of the company was a motivating factor for them to spy on everyone that they felt was rebellious to their twisted company protocols and their prejudicial disorder.

They were pure evil, and they scare me to this day. What would happen if a company or entity like them wrestled control of our society

or a governmental body? They ran a company similar to that in George Orwell's society in *1984*. Nevertheless, a person could quit and become a free man or woman again. However, many people are often nearly trapped in a job. They spent a lot of time at the company, are older, and could not easily leave. Therefore, there are instances where people become stuck with their employers.

Now, with all the new modern-day technologies, unethical and immoral companies like this large publishing company out of St. Louis could become very dangerous.

The technology with its lower prices for surveillance and spy cameras has begun to flood every market. With the rise in crime all over the United States, the average hard-working, law-abiding citizen is tired of being victimized. Therefore, they are arming themselves with small doorbell cameras as well as advanced CCTV cameras and timed infrared-activated recording devices.

So, if you have a strange feeling that you are being watched, chances are you are on camera.