EYES EVERYWHERE

EXPOSING THE CRACKS IN THE GLOBAL SURVEILLANCE WEB

eclipsory
PUBLISHING HOUSE

Eclipsory Publishing House

Committed to Privacy and Truth

eclipsory
PUBLISHING HOUSE

First published by Eclipsory Publishing House in 2025

Eclipsory Publishing House asserts its mission to make knowledge accessible to everyone, promoting privacy, freedom, and autonomy.

Acknowledgments

This book is made possible thanks to the support of privacy advocates who believe in the fundamental rights to freedom and autonomy. Special thanks to these privacy heroes – you know who you are – for ensuring this work can be shared freely.

Printed and distributed by Amazon KDP.

https://eclipsory.com
The Stories They Hope You'll Ignore

This is for those who fight to reclaim their freedom, and for those yet to realize it has been taken.

Preface

In an age where every click, conversation, and action is quietly observed, the line between freedom and control becomes increasingly blurred. The systems of surveillance that govern our lives are often invisible, but their consequences are far from benign. *Eyes Everywhere* is not just a book—it is a wake-up call to uncover these hidden forces and their impact on individuals, families, and societies.

This book explores the erosion of privacy, freedom, and trust in the digital and physical worlds. It draws on real-life examples to show how surveillance systems fail, exposing vulnerabilities that affect us all. From governments using facial recognition to silence dissent to private companies exploiting health data for profit, the stories within these pages reveal the human cost of a watched world.

At Eclipsory, we believe in the transformative power of knowledge. Our mission is to shine a light into the shadows of surveillance, equipping readers with the insights needed to navigate an increasingly invasive reality. This is why *Eyes Everywhere* not only exposes these issues but also provides practical steps to empower individuals to reclaim their autonomy.

This book exists because of the courage and determination of privacy advocates, whistleblowers, and researchers who have illuminated the path to understanding surveillance. To the readers—your curiosity and vigilance are the foundations of change. Together, we can build a world where freedom and privacy are not relics of the past but enduring rights for all.

Thank you for embarking on this journey with us. Your awareness is the first step toward freedom.

— The Eclipsory Team

Contents

Introduction

There was a time when privacy concerns meant you locked your door and shut your shades at night. You asked your neighbor to watch your house when you went on vacation and locked the door to your office when you left work on Friday afternoon. Simpler times in a simpler world.

In 2025, privacy concerns and their accompanying violations have changed just a bit. Your mobile phone provider knows where you are every second of the day assuming you carry your phone with you, which of course everyone does. All sorts of social media platforms and apps go a step further to geo-locate you anytime they want, in order to send you push notifications about things you should consider buying while you're there. New advancements in Artificial Intelligence (AI), which everyone is told is for the good of every aspect of society, don't seem like they're being used for the right reasons.

With a modicum of knowledge, professional cybercriminals and amateur hackers can imitate your social media profile, your voice, and your email address without much of a hassle. So many of our everyday items are connected to the Internet - part of a massive network called the Internet of Things (IoT), but most have very little in the way of security safeguards when it comes to prying eyes. On top of that, we willingly enter our most personal data into form after form and website after website on a daily basis like we're giving breadcrumbs to pigeons in the park. We share our credentials for work databases and streaming services without a second thought, and there are millions of us out there whose password for every major service we use is "Password1".

Every now and again, we get a letter in the mail or a text or an email from some giant conglomerate apologizing to us that our records or data or username or something has been compromised during a data breach. There's always a number to call or a service to contact, but we rarely do it, because hey, it's probably no big deal, right? As a society, we've fallen into a deep trap of not believing the severity of the world around us when it comes to keeping our data and ourselves safe. We consider it a tradeoff for the remarkable technology around us - the ability to talk to our college roommate from halfway around the world on a video screen, the way we don't have to get out our wallet every time we want to order a Starbucks or a new outfit or anything else, the way that our Alexas and Siris seem to just "know" what we were talking about and make suggestions about items we might like to purchase as a result, and the way that cute guy we met just once at some random party are able to find and follow us on social media so easily. At some point, we largely decided that the rewards were worth the risks of all of our fun toys and tools. Of course, that wasn't everyone's opinion. Certainly not that of the small companies who had to declare bankruptcy after having their entire platforms locked down by unbreakable ransomware.

It also isn't the best idea for the people who have had their identities stolen and used to fill bogus medical prescriptions, apply for endless fake credit cards, or take out loans that they're now stuck trying to explain or repay.

And those are just the small potatoes in the grand scheme of things. The tip of the iceberg of what criminals and hackers are up to. What about the 'legitimate' security breaches being perpetrated against everyday people on a routine basis? Anywhere you go and anything you do makes you a potential subject of tracking by some big organization. Whether you're at the airport, a casino, a shopping mall, the bank, or anywhere else, someone is collecting your data. You might not think you're sharing anything worth collecting, but that's unfortunately never true.

What you are spending your money on is of interest to your bank and your credit card companies. Where you're going at the airport and who you're traveling with is fascinating not just to the airlines, but to the government as well. When you're jogging your 5-mile run on Saturday morning, your Fitbit or other fitness device is shooting your health information to one database and the businesses you run by to another, both at a pretty penny. Even if you're using your own money to buy something like expensive wine or a fancy sports car, your bank is filing that information for a future scenario where it might decide you aren't trustworthy enough to receive a loan.

Does it sound like science fiction? Some sort of *Blade Runner,* dystopian future where we're all looking over our shoulders, wondering if we're being followed? The bitter irony is that there's no need to follow us; we've already invited them in. They sit comfortably in our pockets or our purses on our smartphones. They cling to our wrists on our Apple Watches. They watch our children for hours at a time on iPads and video game consoles, and they cozy up to us at home in the form of our thermostats, refrigerators, and AI personal assistants.

At least at work, we are aware our companies are seeing where we go and what we do on the Internet. It's not as nice to learn that anytime we use public Wi-Fi, anytime we walk past a certain type of sensor in a store, and anytime we walk through certain parts of a city, everything from our credit score to our actual face is being considered by a database to see what can be gleaned about us and used to make some sort of decision.

Legendary author George Orwell wrote his seminal novel "1984" in 1949 when his native England was four years removed from the end of World War II. The novel focuses on how truth and facts can be blurred, distorted, and manipulated. For being a 75-year-old novel about a year that came and went four decades ago, that premise is a disturbingly familiar one. We live in a society where every technological advance and the next step away from morality is making it harder and harder to determine what is real and what isn't. While Artificial Intelligence (AI) is becoming more and more the method of delivery of these confusing narratives, they are only happening because people want them to happen and design systems that allow them to happen. A butcher knife in your kitchen doesn't commit murder by itself, it needs a human hand behind it, just as a powerful AI video generator doesn't create a fake video of a political candidate saying they are a Nazi without human hands keying it to do so.

The plot of Orwell's novel involves a protagonist named Winston Smith, working at his country's Ministry of Truth, where his job is to rewrite the events of history so they match up with the state's version of the truth. He works for "The Party", which is led by "Big Brother" —a person with an intense personality cult who uses a force known as the Thought Police to get rid of anyone who isn't in agreement with his policies.

The Thought Police use surveillance, in the form of two-way televisions, cameras, and hidden microphones, to spy on its citizens, even when they are home alone, to detect and eliminate any thoughtcrime. Winston doesn't agree with Big Brother and tries to mildly dissent, having an affair, writing his thoughts in a journal, and joining a group of like-minded individuals, but there are spies at every turn, surveillance equipment of all sorts, and he is both captured and tortured to get him in line with the proper thinking. After being forced into a room containing his worst fear—rats—he emerges as a loyal party member.

While many people read Orwell's work in secondary school or at the college level, even more, know the tale not only from the movie of the same name released in 1956, and rather aptly, a new version in the actual 1984. It received even more acclaim as an advertisement for the Apple Macintosh personal computer that debuted on the broadcast for the NFL's Super Bowl XVIII on January 22, 1984. Borrowing heavily from the novel, the commercial showcases an industrial setting, scores of people marching in a tunnel with large screens on either side, all in black and white with a Big Brother-esque figure giving a speech about “Information Purification Directives”, “Unification of Thoughts”, and being one people with one will, one resolve, and one cause. While that’s going on, a female runner holding a sledgehammer races towards the screen being pursued by four armed and helmeted security personnel thought by most to be Orwell’s Thought Police. The runner launches the hammer into the screen, destroying it, and leads to a voice-over intoning the words, “On January 24th, Apple Computer will introduce Macintosh. And you’ll see why 1984 won’t be like 1984.”

The Big Brother reference in the commercial was a shot at IBM, at the time the absolute leader in the personal computing space. The commercial was directed by Ridley Scott, who also directed the aforementioned *Blade Runner*, *Alien*, and other gritty futuristic movies.

The irony, 40 years later, of course, is that Apple went from the supposed champion of the individual’s rights in the computer age to a huge part of the privacy problem, despite its insistence to the contrary. By limiting its users to mainly its own apps and practices on its hardware, the company forms a circuitous loop that gobbles up data from individuals’ emails, messages, contacts, calendars, photos, backups, notes, reminders, and voice memos. It gets to feel like someone is walking behind you repeating out loud everything that you’re thinking and doing, all day long.

In 2022, after years of big tech getting slammed with controversies over data breaches and shady data practices, Apple released a commercial condemning data brokers. It was called "Privacy on iPhone." The ad featured a young woman watching in horror as her data was auctioned off to a room full of wealthy socialites.

Late-night texts? Sold.

Pharmaceutical purchases? Sold.

Geolocation data? Sold.

Even her entire email history was up for grabs.

Just as it's about to get to the juiciest details, the woman pushes a magic button on her phone, and all of the data and auction buyers vanish without a trace. It's a clever if oversimplified ad, and for Apple's purposes, it does a great job of moving the goalposts so that the impetus is on all those nasty app creators who want to gobble up your data and sell it to data brokers, instead of addressing the real problem—the framework that allows those apps to take your data without restrictions when you install them.

It's a form of dodging blame called privacy washing, where platform and device makers claim they're doing their best to protect user data when that isn't really the case, while shifting the blame onto other companies as the real issue.

In a real-world comparison, imagine Apple as an old-school shopping mall. At some point, mall management puts out a warning that a few of its stores are run by scam artists who will try to rip you off, sell you fake products, and swipe your ID and credit cards when you go in there. While the mall believes it's doing everyone some sort of great service by alerting everyone to the bad practices of those stores, the bigger question is: Why is the mall allowing these bad actors onto its property in the first place?

There are a couple of easy answers to that question and a few more complex ones that we're going to explore throughout this book, but what you're really going to see are a lot of very disappointing patterns of behavior from the powers that be and their allies versus everybody else.

So why write this book now?

It's not just the parallel with "1984" that puts this book in such sharp relief; it's that much like in the novel and its periphery content, we find ourselves living in a world where only some people are vaguely aware of the problem, and all the rest continue to live on in ignorant bliss, believing that all those lovely pings and beeps and trills that signal that someone has done something that they need to be aware of via digital technology are the only things that really matters; and that they are willing to sell their privacy and safety up the river to keep it coming.

The problem is that we stand on the precipice of a point in time where things are about to get much worse, as AI becomes more and more commonplace in the lives of just about every person on Earth. AI can do so many things so quickly that its ability to collect and analyze data must have extreme constraints in place, or risk many parts of our everyday society becoming biased and exploited. Just like every other technology on the planet, without safeguards, AI can be used by bad actors to do really dangerous things; which can pose real-world threats to individuals, companies, and even entire governments. We've already seen AI used for anti-social behavior through spear-phishing, artificial voice impersonation, and fake video releases, not to mention AI algorithms used for human resources, loan approval, and other selection processes that are found after the fact to have an enormous bias from machines that are supposed to be entirely objective. As mentioned earlier, the malaise of it all is perhaps the most worrisome part. It might be human nature; it might be a job of "I need to see it with my own eyes" and it might be simple apathy that keeps us from realizing the Big Bad Wolf when it comes knocking at the door.

When doctors first discovered a distinct, unequivocal link between cigarette smoking and lung cancer, how many people do you think gave up the habit right away? The first report that directly tied the two together came out in 1950 in Great Britain, with a major report in 1954 in the Journal of the American Medical Association which stated that "men with a history of regular cigarette smoking have a considerably higher death rate than men who have never smoked, or men who have smoked only cigars or pipes."[1]

Damning evidence, right? Turns out, not so much. Cigarette smoking increased rapidly in the 1950s and into the early 1960s in the US, with the only ripple going in 1964 when the US Surgeon General put out a similar report advising about the cancer link. But the damage was already done. Lung cancer deaths hit their all-time peak in American men in 1990 and among women in 2002 before they finally started declining. In the 50 years after the Surgeon General's report, the number of cigarette smokers dropped by 50%, but that still means that the other 50% is willing to

[1] Mendes, E. (2014). *The Study That Helped Spur the U.S. Stop-Smoking Movement*. [online] www.cancer.org. Available at: https://www.cancer.org/research/acs-research-news/the-study-that-helped-spur-the-us-stop-smoking-movement.html.

accept the risk of an early, painful death in order to keep smoking.

Think how hard it will be to convince people that all their games, apps, social networks, and smart devices are slowly killing their privacy.

It's not a pleasant thought.

Join us on this journey forward as we expose the problems with big data and look for solutions to stop the slippery slope we're on.

Part 1
Digital Surveillance in Everyday Life

Nobody likes the feeling of being watched. If you look up from your place in line at the grocery store, the airport, or even a bar or a restaurant and see someone else intensely peering at you, it's unsettling. It's one of many reasons we hate being pulled over by the police, pulled out of line at the baggage claim, and summoned to the chalkboard by the teacher. We don't like being watched. We value our privacy.

There are cameras everywhere. They monitor red lights and railroad stops. We see them in banks and courthouses, airports, and government buildings. Plenty of businesses not only have cameras but a big sign telling you that you're being recorded as a little extra bonus of security. A friendly reminder not to do anything stupid, lest you be caught doing so. Those are all security standards put in place for protection against bad actors and possible criminals. They feel it is necessary to protect ourselves against bad things. But what about all the other cameras that are tracking us on a daily basis? What about all the ways that every device we have and every sensor we come in contact with is also registering something about us, 99% of the time without our permission? What about those online records of everything we've ever searched for, bought, or talked about? Should it be possible for anyone, any algorithm, any company, any database to know so much about our lives that they can accurately predict where we are, what we're buying, where we're headed next, and what we're thinking about? That's not just Big Brother, that's full-on "Matrix-level" fears.

For living in the age of information, there is a shocking lack of knowledge about the machines we've so easily turned control of so much of our lives over to. Most people can't tell you how an airplane sustains flight above the ground, much less how an algorithm can predict what they might want to buy next from Amazon based on the flashlight they bought three months ago, or how Google Maps knows exactly where you are while driving through rural Idaho and start pinging you dinner ideas from local restaurants. In this first part, we're going to examine the what, how, and why of some of the most common and commonly misunderstood types of surveillance that are taking place every single day all over the world.

AI-Powered Surveillance

We've all seen the James Bond films or the *Mission: Impossible* sequence or pretty much any procedural TV drama where they show a big room full of monitors and some chief telling the techies at their desks to "enhance" an image repeatedly until they can see the smallest of details and solve some decades-old crime. It's overkill and silly, but every day we get closer to that reality. And it is a frightening one.

First, the stated purpose of using cameras that can achieve facial recognition in public areas is to enhance security and law enforcement. Facial recognition here is described as using AI algorithms to identify people by comparing the captured images to databases that can encompass their social media profiles, any official government photos of them, including their driver's license or criminal record, or really just about anything else. The proponents of using this technology believe it will make cities safer by honing in on repeat offenders and resolving traffic and other incidents more quickly.

But like most digital technology, we seem eager to rely on it far earlier than we should. Such powerful and potentially dangerous technology needs to be tested over an extended period of time, not just thrown out into the field to see what happens.

Detroit's Porcha Woodruff would definitely agree with that statement[1]. In February of 2023, this mother of two, eight

[1] Swarns, C. (2023). *When Artificial Intelligence Gets It Wrong*. [online] Innocence Project. Available at: https://innocenceproject.org/when-artificial-intelligence-gets-it-wrong/.

months pregnant with her third child, was getting her children ready for school when she opened the door to find six Detroit police officers waiting to confront her. She was being arrested, she was told, on suspicion of robbery and carjacking. Who was making such a bold accusation? No one, other than an AI system used by Detroit police to try to match current crimes to former criminals. Woodruff, 32 at the time of the arrest, had been booked eight years earlier when she was 24 because she was driving with an expired license. The AI program matched her photo at age 24 with video footage of the suspect in a recent robbery and carjacking and made the call that this was who the cops were looking for. The victim of the crime also pointed to the 8-year-old photo when viewing a lineup of suspects. That apparently was enough to arrest Woodruff in front of her children, ages 12 and 6, that morning. Woodruff thought it was a joke at first, mentioning to the officers that the odds of an eight-month pregnant woman performing a carjacking seemed a little odd, didn't they think? They responded by taking her to jail and leaving her in a cell for 11 hours while they processed paperwork which included an outlandish bond set at $100,000—meaning she'd have to get together $10,000 just to get out. Telling jail personnel that she suffered from gestational diabetes didn't move the needle, nor did the stress-related contractions she started experiencing late in her incarceration. She was rushed to the hospital immediately after being released but fortunately did not lose her baby.

Woodruff, working full-time as an aesthetician while also attending nursing school, never even had to go to court. A prosecutor dismissed the case a month later due to the lack of evidence. But Woodruff wasn't going to just let it pass. In the summer of 2023, Woodruff filed a lawsuit against the City of Detroit. Among the information revealed in the filing was the fact that the AI system intentionally used a photo of Woodruff from her 2015 arrest, even though it also had a 2021 driver's license on file. Woodruff was the sixth person of color wrongfully arrested since Detroit started using facial recognition software, and it's not exactly a new development. Dating back four years before the incident with Woodruff, federal researchers filed a report about the huge problems with racial bias in close to 200 facial recognition algorithms[2]. Most glaring errors came to identifying people with darker skin colors—Blacks, Hispanics, and Native Americans in particular. One of the researchers of the 2019 report, Patrick Grother, stated that "compared to their performance against whites, some algorithms were up to 100 times more likely to confuse two different non-white people."

The same report showed that Black women were the most likely to be misidentified by the FBI's mugshot database. Woodruff, a Black woman herself, sued the City of Detroit and one of her arresting detectives for false arrest, false imprisonment, and a violation of her Fourth Amendment rights to be protected from unreasonable seizures—the police took her phone and did not return it upon her release, claiming they needed to check if she was in the area, even though they had not obtained a warrant at the time of her arrest. It was the third time the City of Detroit had been sued over an AI-related misidentification. In 2019, the city

[2] Fung, B. (2019). *Facial recognition systems show rampant racial bias, government study finds*. [online] CNN. Available at: https://www.cnn.com/2019/12/19/tech/facial-recognition-study-racial-bias/index.html.

revised its guidelines to only use the tech for violent crimes and/or home invasions.

In August 2023, Detroit's Police Chief James White finally spoke to the media but refused to throw the AI system under the bus, instead blaming his human officers.

"I have no reason to conclude at this time that there have been any violations of the DPD facial recognition policy," the chief said in a press conference. "However, I have concluded that there have been a number of policy violations by the lead investigator in this case."

According to White, the photo of Woodruff was one of several delivered by the AI, and the detective then used it in a lineup, which is against department policy.

If Woodruff's story sounds familiar, it's because the incident was a near carbon copy of one three years earlier, also in Detroit. Robert Williams, a black man, was arrested on his own property in Farmington Hills, Michigan, in front of his wife and two daughters for a crime he had nothing to do with. He had been identified as the person responsible for stealing designer watches from a boutique store in Detroit.

Williams' expired driver's license photo was identified by AI as being the thief based on video footage, and his picture was also put in a lineup, and identified by a witness who didn't even see the crime happen. Williams spent 30 hours in jail, missing his oldest daughter losing her first tooth, and the charges were dropped within a month. Williams also filed suit against the city and was awarded $300,000, and his story received such acclaim that he wound up writing an opinion piece for Time Magazine about it[3]. It took more than four years for Williams to be awarded the money by a federal court. As of November 2024, Woodruff's case vs. Detroit and the Detroit Police Department was still in court.

[3] Williams, R. (2024). *Why Police Must Stop Using Face Recognition Technologies*. [online] TIME. Available at: https://time.com/6991818/wrongfully-arrested-facial-recognition-technology-essay/.

AI Camera Surveillance Worldwide

The use of AI cameras in ways that seem to violate our basic liberties and freedoms is not limited to the Detroit police or even to the United States. The situation in Detroit seems mild to what is going on in China, which is apparently trying to corner the market on becoming the literal "Big Brother" as fast as it can. The AI facial recognition use in big cities like Beijing has been in place for almost a decade, with sophisticated algorithms running that can identify when someone is 'unfurling a banner', which typically means some sort of political statement is happening.[4]

The AI in those cameras is made by a company called Dahua Technology. It is sanctioned by Western governments, even as Dahua has tried to hide proof that it even exists. When asked for details by IPVM, a surveillance research company, Dahua responded by deleting references to the AI system known as Jinn from its website. Ironically, a little extra snooping by IPVM uncovered archived versions of the website where the Jinn system is described as being used for "social governance" and "social safety".[5] According to those web archives, Dahua launched Jinn in 2021. It should come as no surprise that this came after an extremely turbulent last few years for the world's Asian superpower.

The banner-unfurling algorithm is likely a direct response to the 2022 incident when a protestor in Beijing hung two

[4] Radio Free Asia. (n.d.). *In China, AI cameras alert police when a banner is unfurled*. [online] Available at: https://www.rfa.org/english/news/china/surveillance-06052023142155.html.

[5] Ibid.

giant banners off the overpass of a freeway as the Chinese Communist Party's 20th National Congress was about to kick off in October 2022. One read, "Remove the traitor-dictator Xi Jinping!" and the other said, "Food, not PCR tests. Freedom, not lockdowns. Reforms, not the cultural revolution. Elections not leaders. Dignity does not lie. Citizens, not slaves." The man, identified as Peng Lifa, has not been seen since being arrested shortly thereafter. The country's intense Internet censorship cracked down on any mention of the man, the banners, and even the district they were hung in, on Chinese's social media and search engines. Even a pair of older rock songs that were played by radio stations in reference to the act were wiped out of existence online.

AI is one of those technologies that China has targeted as a key to its future spot as the world leader and is tabbed for rapid success. The country started deploying AI in 2017 and wants to take over from the US as its global hub by 2030. That might be true for government spending, but private investment in AI in the US is off the charts.

Cracking down on banner hangers is hardly the Chinese government's worst crime. There is strong evidence that China is using AI facial recognition to detain Muslim Uyghurs in the Xinjiang region. The Uyghurs are Turkic-speaking people who have been imprisoned in the millions by China since 2017. Among the crimes the government is accused of leveling these people based on more than their ethnicity include religious restrictions, forced labor, forced sterilizations, and surveillance[6]. These people hail mostly

[6] Maizland, L. (2022). *China's Repression of Uyghurs in Xinjiang*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/

from China's border countries like Kyrgyzstan and Tajikistan.

The Dahua technology has been officially sanctioned by the US, Australian, and Great British governments. It is said to use biometrics data to surveil everyday citizens. This is on top of other surveillance algorithms in place in China. For instance, if a person with a criminal record, even decades in the past, checks into a hotel, the local police station is alerted. In addition to the aforementioned Uyghurs, AI is being used to seek out the following population segments. No, it's not a joke.

- Foreigners with illegal residence status
- Staff members of certain universities
- Faculty of certain universities
- Foreign journalists
- Foreigners who have visited Xinjiang or similar provinces where Uyghurs live
- Individuals who have/have not been given COVID-19 vaccines
- Suspected criminals
- Known sex workers
- Known drug dealers
- Families suspected of using too much electricity

These are just the tip of the iceberg of a full 26 target populations that Shanghai has listed as 'target populations', which means they are being watched. Others include

backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights.

people with psychosocial disabilities and people known to file petitions against the government.

Records indicate that in the early days of Chinese surveillance, the algorithms were reporting people who suddenly started the habits of smoking or drinking, or purchasing items used to make a tent—suggesting they were preparing to live 'off the grid'.

The cameras aren't hidden out of the way, either. In popular public places, they are mounted like traffic lights, with multiple cameras turned at multiple angles to capture every bit of the scene.

The Chinese government has gotten more extreme in its attempts to quell political rallies and other protests that spiked between 2020 and 2022 based on the nation's response to the threat of COVID-19. After realizing that the virus had escaped Wuhan in late 2019, it enacted a "Zero-COVID" approach that lasted until the end of 2022. This approach included forced isolation of patients, censorship of anyone suffering from its symptoms, ejection from the country of any foreign journalists, canceling Chinese New Year celebrations across the country, and a declaration of emergency that let the government do whatever it wanted to carte blanche. A month of protests by the citizens of China occurred in November and December of 2022 which finally resulted in the abandonment of the zero-COVID policy, but also had many protestors detained, censorship running wild, and raised tempers all over.

Hearing that China is monitoring its citizens for behavior, not in line with its policies is not exactly breaking news. The fact that something similar is happening in a Western stronghold like London is far more ominous.

It wasn't until June of 2024 that information came out that Network Rail Limited, the infrastructure manager of almost all of Great Britain's railway network since 2002, had been capturing unauthorized pictures of train passengers to analyze their emotions via AI cameras at major London stations dating back to 2022[7].

The news was very aptly broken by a civil liberties group called Big Brother Watch. Network Rail wasn't the only complicit body in the violation; Amazon's recognition software was used to detect emotions including happiness, sadness, or hunger. This was implemented at major stations like Waterloo, Glasgow, Leeds, and Reading, where the AI system also recorded the genders and age ranges of each passenger. After being made aware that Big Brother Watch had used a Freedom of Information request to get access to the information, Network Rail first said in a public statement that analysis was being done to "measure satisfaction" but later admitted that it was also intended to "maximize advertising and retail revenue."

The company further claimed that the AI trial was also intended to address issues such as bicycle theft, trespassing, overcrowding, and slippery floors. Why the company would need to know that someone is a 55-year-old woman who appears hungry to determine if a floor is slippery or not remains anyone's guess.

Big Brother Watch spokesman Jake Hurford told British

[7] Lancefield, N. (2024). *AI cameras used at London stations to detect passengers' emotions without them knowing*. [online] The Standard. Available at: https://www.standard.co.uk/news/london/network-rail-ai-cameras-train-stations-london-euston-waterloo-b1165407.html [Accessed 19 Nov. 2024].

media: “It is alarming that as a public body, it decided to roll out a large-scale trial of Amazon-made AI surveillance in several stations with no public awareness, especially when Network Rail mixed safety tech in with pseudoscientific tools and suggested the data could be given to advertisers. Technology can have a role to play in making the railways safer but there needs to be a robust public debate about the necessity and proportionality of tools used.”

Alarmingly, Network Rail isn’t the only British transportation manager using secret ways of recording travelers without their knowledge. In February 2024, Wired revealed in an article that Transport for London was using a computer vision system without anyone’s knowledge.[8]

Given that the London Underground can routinely carry four to five million people per day, this is a gross use of power that should never have been rolled out without informing the public. The machine-learning software combines with live CCTV footage in an attempt to “detect aggressive behavior, spot guns, knives, and look for people who are dodging ticket lines, or who have fallen on the tracks.”

In one of the documents obtained by Wired, an algorithm at Willesden Green station that averaged 25,000 passengers per day before COVID was set up to look for people in wheelchairs, people pushing babies, people vaping, people accessing unauthorized areas, and people getting too close to the platform edge. In a follow-up, partially redacted statement, the study showed that the algorithm made frequent

[8] Burgess, M. (2024). London Underground Is Testing Real-Time AI Surveillance Tools to Spot Crime. [online] WIRED. Available at: https://www.wired.com/story/london-underground-ai-surveillance-documents/

mistakes: identifying children following their parents through the turnstile as line dodgers, flagging people for stealing bikes when they were just folding them up, and failing to notice when two police officers, as part of the experiment, walked past the CCTV holding a gun and a machete.

From the Detroit police to China to London, there is a very clear-cut line of similarity we're seeing here, and that's the fact that not one person is giving permission to have their image captured and analyzed while they are in a public place. The responses from the Detroit police and the English transportation authorities explaining their actions come across very much as organizations that know that if they ask permission before embarking on these trials and rollouts, they will be met with staunch public criticism and debates that will make it difficult to go forward with them. It very much feels like the childhood mantra of "beg for forgiveness rather than asking for permission", except that nobody is forgiving these large-scale powers for violating basic rights and intrinsic desire for privacy. Even worse, these are just the examples of a few that have gotten caught using AI cameras without public knowledge or getting sued when they detained an 8-month pregnant woman for carjacking based on an 8-year-old picture that a computer saw.

Who else is out there recording our images as we go about our days?

The cameras in London are supposedly able to read our emotions, meaning they are trying to figure out what we are thinking. Isn't the next step to determine what we might do next and detain us before we can? That sounds disturbingly like 21st century science-fiction in the form of Steven Spielberg's "Minority Report" and Marvel's "Captain America: The Winter Soldier." The former is based on the Philip K. Dick novella of the same name, taking place in 2054, and sees Tom Cruise working in the "Pre-Crime" unit of the Washington D.C. police department where criminals are apprehended before they commit crimes using special technology.

In the latter, the US's strategic homeland department is revealed to be using satellite technology to eliminate threats against the government preemptively in the ultimate heel turn by actor Robert Redford. Named "Project Insight", the list of threats includes every superhero, known or unknown, as well as many well-regarded scientists and politicians. It's very disturbing how quickly life is imitating art in this form.

Smartphone Tracking

We get a certain sense of security when a new app on our smartphones asks if we want to let it use our location "this time only". "Only when running this app", or "always". It makes us feel like we have a sense of control over how our data is being used.

We don't.

While neither company was thrilled to let the truth out, it is undeniable that both Google—maker of the Android operating system, and Apple—maker of the iPhone are able to keep tracking your phone's location and plenty of other things even if you have your tracking permission settings turned off. The jig was up for Google in 2018 when a report by the Associated Press revealed that turning off your Location History might feel good, but it can't stop the invasive powers of Google itself on both iPhones and Androids. Google circumvents its own promise by using its weather updates to track where you are, pinging the cell phone tower nearest your location when you do a search on Google, and snapshotting your current location when you open Google Maps—not even using it to look something up, simply opening the app.

The cat was out of the bag thanks to a graduate researcher from UC-Berkeley who had turned off her location history on her Android phone and then got a notification from the app asking how she enjoyed her trip to Kohl's, which the phone should not have known about.

Even after its very forward conversation about turning off your Location History, Google had to go back and revise that message and show that the only way, supposedly, to turn off everything would be to go to the "Web and App Activity" setting and turn everything off for all your mounted apps.

It's funny how they didn't mention that part the first time around, isn't it?

Of course, Apple and Google are hardly the only culprits here, although they are two of the largest information companies in the world and seem willing to do almost anything to keep it that way.

The simple fact is that nearly every app out there, with few exceptions, wants to track every single second you spend using their product—and, if they can get away with it, as much of your time when you aren't using their product as possible. Your data allows them to improve their app, find new people to market to, and make more money. That's all this is for a lot of companies.

Sure, they'd like the app to work ten percent more efficiently, but mostly, they want it to work better so more people will rely on it—allowing them to charge their advertisers, subscribers, or other paying users more per click and ad.

The real point here that most people fail to grasp is that while most apps are good tools or good forms of entertainment, they are also really good trackers. Every time you open them up, they're devouring stuff about your identity, your preferences, your location, your purchase habits, your financial information when making those purchases, what hours you're most active, and so on down the line.

And while you might first wonder why Words with Friends or Uno needs so much of that data, the answer is that they actually don't. But buried in the code you can't see on the app that just slid onto your phone is a very subtle connection that lets the app send data straight to the likes of Microsoft, IBM, Verizon, X, Facebook, Google, Amazon, and so forth. It's sort of like the little apps are the fishers in a village who go out each morning to collect oysters from the tidepools. They want the creatures for the meat that they provide in order to stay alive.

Those shiny little pearls inside are worthless in their economy, but priceless when they sell them on to exporters who will make them into jewelry. Your data is the pearl in the oyster shell. Not worth a ton to your tip calculator app, but a pretty penny when sold up the river. They get away with this through all sorts of technical jargon to confuse you about what they are doing, and a lot more that they just don't mention at all. For instance, when apps say they are tracking you, that doesn't mean they are checking your location, but rather that they are recording everything that you are doing, your behavior, your choices, anything you buy in the app, what times of day you're using it, how long you're using it for each time and so forth. Those apps are treating you like Jane Goodall watching chimpanzees: collecting every shred of data to be used later to make inferences about your future behavior.

Not exactly the best time to be monkeying around, is it?

Some apps don't even pay attention to what you're doing on their app. They're able to see what else you're doing—like what apps you're opening when you shut theirs down, or your physical location when you get on their app—meaning they know if you're using it at work, at school, at home, at the airport, or anywhere else.

Apps use any number of technologies to track you. Despite their small size, this can include cookies, tracking pixels, GPS/location services, social media integration, analytics, requesting permission, and device identifiers.

How do we limit this data exposure? Because we all know we aren't giving up our smartphones or our convenient world of apps any time soon. There are no foolproof ways to keep all your data safe, but a number of the following can keep a lot of uninvited guests from burying their noses in your data and gorging themselves on what they find.

- Use Multi-Factor Authentication for your accounts: It's not brain surgery to guess your 4- to 6-digit passcode on your phone or the one password that you use for all your accounts. MFA means that you're putting a hacker through the wringer to get to where the good stuff is.
- Use trusted Wi-Fi networks: One of the oldest scams in the book is logging into a Wi-Fi network that seems like it's probably legitimate only to realize some third party is devouring everything you put into the keyboard.
- Use a VPN: Virtual private networks are really smart options for covering your bases online when you want to secure what you're searching for, writing, texting, or anything else.
- Don't download apps from unknown developers: Just because they are on the iPhone or Google Play store doesn't mean they're safe! Check who made them, what country they're from, and who originally published them. If it's some shell company that is owned by Alphabet or Meta, go

ahead and assume that your information is going right to their database as soon as you open the app. Don't be fooled by clones and knockoffs of the real thing. Micro Touch is not Microsoft.

- Avoid clicking links suggested by your apps: They might go somewhere fun or interesting, but they likely also go somewhere that is going to phish your information or install tracking malware on your phone. Phones are woefully inept at realizing when there's a virus present. You're more likely to figure it out because your phone is overheating from so many processes running before you get any sort of notification that something is off.

Social Media Privacy Breaches

For proponents of minimizing their digital footprint and those who have been living off the grid since before there even was a grid, imagine the horror of watching people you care about mindlessly type in every piece of personal data they have into the likes of Facebook 20 years ago, in order for the algorithms to sift a little better in finding every single person they've ever known in order to be better 'connected' with each other. What seemed like fun and games a couple of decades ago is a lot more of a real situation now. We've all learned the hard way that not only did Mark Zuckerberg not want to accept our friend request, but he also wanted to gobble up our data like a hungry beagle at dinner time—selling it all out to the highest bidder while also using it to feed you just the right ads to keep you staring at Facebook for the rest of your life.

Facebook has been the wunderkind of social media ever since Zuckerberg unleashed it on the Harvard College campus more than 20 years ago on February 4, 2004. Pretty much every step of its history for the next 15 years felt a bit like the story of King Midas; everything Zuckerberg and his friends touched seemed to turn to gold: Tagging, newsfeed, the mobile app, the Like button, acquiring Instagram, going public, being the first social media site to hit 1 billion active users, acquiring WhatsApp, and so forth.

The carriage started turning pumpkin in 2018 when Facebook started getting lumped in on tags with a name that it would come to rue for a long time: Cambridge Analytica. Cambridge, founded in 2013, had a tool that allowed one application to access the features/data of another. For the social media development crowd, it was big news, because it meant that all of their likes, trends, and posts could theoretically be analyzed, and future marketing, sales, and strategy decisions could be made based on what was found.

On March 16, 2018, Facebook abruptly announced on its own website that it was suspending Strategic Communication Laboratories, including Cambridge, from using Facebook. The press release read that in 2015, Facebook learned that Dr. Aleksandr Kogan from the University of Cambridge had lied to them and violated their Platform Policies by passing data on from Facebook.

Now, the curious mind would ask why, if Facebook had made this discovery about the lying in 2015, why was it only suspending the parties involved and admitting what had happened three years later?[9]

That question was answered swiftly and painfully a mere 24 hours later when The Guardian and The New York Times teamed up to break a story about a whistleblower working for Cambridge Analytica who said the company had used 50 million Facebook profiles to model their algorithm and had done it with Facebook's knowledge. It was a bomb blast to the face for the always-cool, unflappable Facebook, and made the sudden flurry of retro-history the day before seem painfully planned. Zuckerberg lashed out repeatedly at the media for calling what Cambridge did a "data breach" since they hadn't actually hacked anything or stolen the data. Some talking heads countered that this was quite a bit worse—they stole the data with Facebook's willing assistance.

[9] Grewal, P. (2018). *Suspending Cambridge Analytica and SCL Group From Facebook*. [online] About Facebook. Available at: https://about.fb.com/news/2018/03/suspending-cambridge-analytica/.

Despite Facebook's many attempts to try to make everyone feel like it had everything under control and would swiftly fix things to be better, the fact that it had happened and that Facebook had known about it for at least four years brought the harsh scrutiny of the government on the social media king. Just a few months later, Zuckerberg found himself not in front of a live chat or a hackathon, but the US Committees on the Judiciary and Commerce, Science, and Transportation in the Capitol Building.

By the time the hearing started, it was revealed that the actual number of users that Cambridge had gotten ahold of was 87 million, not the original 50 million. Some of the sharper-minded members of Congress who spoke that day also voiced concerns that Facebook itself could simply harvest all the data that it collected and sell it to anyone it wanted for a huge profit.

But instead of getting the sharp-witted, "smartest guy in the room" persona that many had come to associate Zuckerberg with, perhaps in large part due to the movie "The Social Network", this version of the boy billionaire seemed unprepared, vague, and fairly unhelpful, with answers including:

- "Long privacy policies are very confusing, and if you make it long and spell out all the details, then you're probably going to reduce the percentage of people who read it and make it less accessible to them."
- "We should have followed up and done an audit (in 2015), that's not a mistake we will make (again)."
- "We try not to make the same mistake multiple

> times, but in general, a lot of the mistakes are around how people connect to each other."

He also said he had no knowledge of what Facebook was doing in favor or against Donald Trump's 2016 presidential campaign, he did not know specifics about whether Facebook Messenger kept records of calls and texts written by minors ages 13-17, and that he did not know if Facebook could track a person's Internet history. He also said that Facebook didn't "feel like a monopoly" to him despite being unable to name a single competitor in the social media space that Facebook had not bought.

Zuckerberg's performance was met with outright contempt from the news media, with The Guardian running an opinion piece calling it "an utter sham."[10] Zuckerberg refused to appear before the British parliament. He had to appear in Congress again in 2021 to address concerns about Facebook's role in the legal immunity the law gives social platforms and Facebook's role in the January 6, 2021 attacks on Washington D.C.

He was there again in 2024 to be questioned about the role of child safety on social media platforms. While continuing to stick to his vague "do better" mantra, he did apologize in general to the families of children who had suffered harm or abuse by way of Facebook.

So, how do social media platforms get so much of your data? And why? The why is the same painful answer we keep

[10] Teachout, Z. (2018). *Mark Zuckerberg's Facebook hearing was an utter sham | Zephyr Teachout*. [online] the Guardian. Available at: https://www.theguardian.com/commentisfree/2018/apr/11/mark-zuckerbergs-facebook-hearing-sham.

arriving at: for money and power. Facebook can sell more targeted ad space to companies that are going to line up with exactly what Facebook users want based on their behavior and preferences. Moreover, political parties—some of the richest organizations in the world—want to dig their hands deep to influence the most important voters for each new election cycle. The simplest truth is that we not only allow them in; we invite them because we crave the full monty—the highly personalized experience that makes us feel like the center of the universe, with everything catered directly to us at all times.

Social media and other parts of the Internet make that easy and even cool. We sign into Facebook and get greeted by name, followed by a news feed of items that are all tailored and made for your interests, a list of what your friends are up to, what your favorite brands are up to, your favorite TV shows, your favorite movies and your favorite gossip. By the time we've scrolled through it all, Facebook has gathered yet another massive collection of our data, running it through its filters to refine our profiles even further.

We are so used to simply tapping 'Accept All' whenever a cookie warning pops up that we click it almost instinctively —just to get to the good stuff faster. We never stop to read where that data is going or who will see it. But cookies are just the beginning. Companies track your data through browser fingerprinting, geofencing, cross-site tracking, and a host of other clever, invisible techniques. So, the next time you think it's a weird coincidence that your Alexa shows an ad for cookie dough after you clipped a coupon for cookies on your phone, remember: it's never a coincidence anymore. It's a network of like-minded, interconnected devices bouncing your information around like a beach ball.

We've hit on Facebook pretty hard in this chapter, but what about the other luminaries in the social media constellation? Twitter, Instagram, and TikTok in particular have all had their run-ins with the law and the moral law of man over the years. TikTok is constantly in jeopardy of being banned in the United States due to its Chinese ownership. The company ByteDance owns TikTok, which currently has around 170 million US users. As we've seen earlier in this chapter, however, the Chinese government has a way of getting what it wants from anyone in China. Many in the US government and other groups fear that ByteDance could be forced to hand over personal information on hundreds of millions of US citizens to China for their own nefarious purposes. Near the end of his term, President Joe Biden signed a deal to allow TikTok to be sold to a non-Chinese company and stay legal in the US. As of the writing time of this book, ByteDance had until January 19, 2025, to make the deal happen. With President-Elect Trump back in office, whether that deal stays on the table is anyone's guess.

Beyond the China issue, TikTok is ripe for data breaches because of the nature of the beast. Everything on TikTok is done in video/audio format and people often share their personal information, which can be easily screenshotted or recorded and then shared without permission. X (Twitter) and Instagram have many of the same problems. Instagram might be the most precarious of the four major platforms because of its real-world danger element. People often check in their location when they are out and about, at restaurants, at bars, and plenty of other places. Many people are smart enough to share that information only with those they truly know and trust on the platform. Others, however, make it visible to anyone—leaving them vulnerable to in-person encounters that range from annoying to awkward to downright dangerous.

In November 2024, the University of Florida head men's basketball coach came under a sexual harassment investigation in which multiple current and former Florida female students reported disturbing behavior from the coach on Instagram.[11] Police reports showed that Golden was accused of cyberstalking, sexual harassment, and sexual exploitation over a period of more than a year. Part of the complaint against him is that he would "like" Instagram posts by women when they checked into a location on Instagram, take photos of them walking or driving in the area, send the photos to the subjects, and in some cases, persistently message them on Instagram saying he was in the area and they should get together. A 2021 report found Instagram to be the "most invasive app"[12], collecting 79% of its users' personal data and sharing it with third parties. This data includes, but is not limited to: search history, location, contact list, and even financial information. Facebook finished a fairly distant second on the list at 57%, with LinkedIn, YouTube, and food delivery app Uber Eats also scoring poorly.

One of the biggest shake-ups in social media over the past

[11] Rorabaugh, D. (2024). *Florida basketball's Todd Golden under sexual harassment investigation. What is Title IX?* [online] Tallahassee Democrat. Available at: https://www.tallahassee.com/story/sports/college/2024/11/15/todd-golden-florida-basketball-coach-sexual-harassment-accusations/762343030007/ [Accessed 20 Nov. 2024].

[12] Cuthbertson, A. (2021). *Instagram is 'most invasive app', new study shows*. [online] The Independent. Available at: https://www.the-independent.com/tech/instagram-invasive-app-privacy-facebook-b1818453.html.

few years has been the purchase of the former Twitter by billionaire tycoon Elon Musk for $44 billion in October 2022. Changing the name, the format, and putting in price tiers while also firing a legion of staff haven't made Musk very popular in the X community, but things got even worse in October 2024 when Musk announced a change in the company's privacy policy to allow third-party apps to train AI models on X data—specifically user posts. This means that any personal data, happy birthday photos, videos, or anything that a user post can be used to train AI. There is an opt-out option according to Musk, but the new policy update didn't bother telling users where the controls are to make that happen.

Data Brokers and Online Tracking

We understand why tech giants like Google, Facebook, and Amazon are gobbling up our data like so many Pez on Halloween. But the truly nefarious players in this business are companies most people have never heard of, let alone understand, like Acxiom and Experian.

Acxiom describes itself as a provider of 'data, identity solutions, and people-based marketing solutions,' while Experian—best known for its credit reports, calls itself a multinational data analytics and consumer credit reporting company. Those are just polished labels for what they really are: data brokers. They collect massive amounts of personal consumer data and sell it to an endless list of buyers, who then use it to shape nearly every aspect of their financial, marketing, and sales strategies for the years ahead.

In 2022, the data broking business was worth $200 billion a year, with more than 4,000 companies involved in the practice.[13] Their main sources of data include your web browsing history, public sources like government records, commercial sources such as the things you've bought, and nearly anything tied to a coupon or loyalty program.

But the most troubling source of all? Our consent.

As we've mentioned a number of times, we give consent without even blinking an eye when we install an app, sign up for a reward card, or anything else in which we are trading our information for some sort of perk or prize.

[13] Newsweek. (2016). *There's very little oversight in the industry of data brokers*. [online] Available at: https://www.newsweek.com/secretive-world-selling-data-about-you-464789.

And what do these brokers collect? At the bare minimum, the list includes:

- Name
- Address (current and previous)
- Birthday
- Gender
- Marital status
- Family status
- Social security number
- Education level
- Assets
- Occupation
- Phone number
- Email address
- Buying habits
- Personal interests and hobbies
- Income level
- Prescription medications
- Political views
- Criminal record

And more things every day as we integrate more and more of our lives into our online apps and platforms.

The data is used for marketing and advertising purposes, for risk mitigation, for health insurance, and to populate People Search sites. In 2022, Nick Berk published a fascinating in-depth look at data brokers on Medium by obtaining his own data report from Experian and Acxiom[14]. He received an

[14] https://medium.com/@nick.berk/i-asked-two-data-brokers-what-they-know-about-me-what-i-learned-and-how-new-laws-made-it-possible

18-page PDF from Experian and 22 pages from Acxiom. He found the reports both disturbing but also misleading, proving once again that these powerful algorithms that companies are unleashing on all sorts of big-world problems are flawed and definitely need more testing. For example, Experian thought he was 'highly likely' to be interested in luxury women's retail shopping, which he quite obviously is not. Acxiom was similarly all over the board with his finances. It guessed he had a net worth between $11,000-$11.3 million, and between $1,000 and $2 million in bond holdings.

Experian had detailed information about multiple purchases he had made in the past six years. There were large-scale flaws in both reports, including one saying he has three children (he has none), that he is Protestant (he isn't), and that he had spent $102 online in the past four years (he spent more).

So, while we can hem, haw, and shake our fists at how much data the social media platforms are swiping from us, it is a good idea to realize that these powerful brokers are the real major players in the data game.

Part 2
Government and Corporate Surveillance

As nerve-wracking as all the examples of social media and transportation hubs spying on us through cameras, our phones, and our Internet searches are, the real elephant in the room, and the true version of Big Brother for most—is the sort done by our governments and our workplaces. Seemingly every time a new set of government documents is declassified, we learn more disappointing truths about the powers that we've elected to run our countries. For example, the US government has apparently been studying UFOs for years despite always pretending everything was a wayward weather balloon or the fact that in the late 1970s, the US almost started World War III because a few people at NORAD mistook a simulation of a Soviet surprise nuclear launch for the real thing.[1]

Much like our friends at Facebook and their ilk, a lot of

[1] The (2015). *Paleofuture*. [online] Paleofuture. Available at: https://paleofuture.com/blog/2015/2/16/the-computer-simulation-that-almost-started-world-war-iii [Accessed 20 Nov. 2024].

what the government does is intended to not only keep the power that it already possesses but also find ways to expand that power as much as possible without causing some sort of revolt among its citizens. When we delve into corporate surveillance a bit later in this section, we'll explore some rather disappointing similarities between how our governments and our bosses think of us and trust us about as far as they can throw us.

If you're old enough to remember the terrorist attacks of September 11, 2001, fairly well, then you're likely also aware that sweeping changes in US policy came immediately thereafter. The Department of Homeland Security was created, but some of the powers that it was given, and some that were rapidly expanded to other departments at the federal level were more than a little unnerving when it came to an individual's rights. Just six weeks after the attacks leveled the World Trade Center and the Pentagon, and claimed the lives of more than 2,000 people, the US Congress passed the USA Patriot Act. It was 131 pages long, did not have a single amendment to it, and had virtually no debate over the contents of it. The official name of HR 3162 was "United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." After watching memorial after memorial for firefighters, cops, first responders, and the brave souls in the buildings and on the airplanes, who in their right mind would object to something like that?

The problem was that in a desire to hunt down terrorists on foreign soil and domestic so that America never went through another such dark day, it gave federal law enforcement services almost unlimited power in what they could do with any sort of justification, including:

- Tapping into domestic and international phone lines without a warrant
- Authorizing indefinite detention without trial for immigrants
- Permission for law enforcement to search property and records without the owner's consent or knowledge

That is a shocking amount of freedom taken away in a really short amount of time. Essentially telling everyone in the country: Your basic rights no longer exist if any member of law enforcement is suspicious of you; and if you're an immigrant, your rights are completely out the window.

Doesn't exactly sound like the good ol' US of A, does it?

Not surprisingly, many liberties were taken and continue to be taken by the Patriot Act and the creation of the Department of Homeland Security. Some of the more severe ones have been exposed and some parts of the legislation repealed, but for the most part, you can't unring the bell. Once an organization gets a taste for that sort of power, there's no putting the genie back in the bottle.

Don't believe it? You don't have to look much further than the US' PRISM program enacted by the National Security Agency (NSA) in 2007 to see how it has evolved since the grievous days following September 11. PRISM is the code name for a program that allows the NSA to collect all Internet communications from any US-based Internet provider that matches certain court-approved search terms. PRISM then targets specific communications that travel encrypted along the Internet in order to pay closer attention to who is saying these things and what is being said.

If all this sounds vaguely familiar, you're likely familiar with the name Edward Snowden. Snowden, an NSA contractor, leaked the existence of PRISM in 2013, more than six years after it was given life by President George W. Bush's Patriot Act and overseen by the US Foreign Intelligence Surveillance Court. There's a lot to unpack there. First of all, why is the US Foreign Intelligence Surveillance Court overseeing something that is defined as being all US-based Internet communications? Second, why was this program kept a secret for six years when American tax dollars are paying for every last penny of it?

Third, why does it take a whistleblower at the peril of his own reputation and safety to let us know that some secret court somewhere is deciding what words might get us followed home by the NSA if we type them in an email or a search engine? If a college student is writing a term paper on terrorist cells and how they procure chemical compounds to make bombs, are they going to get dragged to their dorm room at 4 a.m. one morning for questioning?

Heck, will the same thing happen to me typing those words into my Google document, when I know my ISP is one of the ones that falls under PRISM's program?

Perhaps the most troubling part of this is that the reasoning for the program is the government deciding for everyone what is safe and what isn't, and determining who might be a threat—not based on crimes they commit, but on what they do in the privacy of their own device.

It sure sounds a lot like China scrubbing its search engine results and social media networks of key terms following the emergence of the banner-hanging protest in Beijing that we discussed in Part I. Ask any American politician who approved the Patriot Act of law enforcement agent from the NSA and you'll get loud, long laughter if you suggest that our tactics are quite similar to those of China. Yet, when you line up the secretive nature of the programs and the idea that there is no public knowledge of how they work, suddenly yet another book by George Orwell comes to mind - "Animal Farm." At the end of that parable, the pigs have taken control of the farm from the men, but wind up inviting other men to come and have dinner and talk about investing in the farm. As the other animals look through the window at the two groups of greedy individuals, they realize they can no longer tell porcine from humans. If our way of life is so very different from China's, why are we enacting the exact same type of 'secret police' tactics to target people based on what they are typing? The government continues to claim that PRISM is there to protect against the real threats, but if that is the case, why did it find the need to order a subsidiary of Verizon to turn over logs tracking every single one of its customers' telephone calls in 2013?[2]

Does that mean the NSA was accusing millions of people of being terrorists; or did it just see how much it could get away with?

Not to be outdone, China has created a system that actually ranks its individuals and businesses on how trustworthy they are. It's sort of like a list of who the popular kids are in school, except the further down you are on this list, the

[2] Greenwald, G. (2013). *NSA Collecting Phone Records of Millions of Verizon Customers Daily*. [online] The Guardian. Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

more likely you are to just vanish one day and not be seen again for months - like the case of Bao Fan, a Chinese investment banker/investor who founded the powerful bank, China Renaissance. After surviving an anti-corruption investigation in 2022, Bao went missing in February 2023, causing his company's stock to drop by 50%. It was later revealed that he was in custody of the Chinese authorities as part of an investigation into one of his former colleagues. As of this writing in the latter stages of 2024, Fan has resigned from all of his positions at the bank and has not been seen in public since the vanishing[3].

In the US and many other countries, a credit score measures how likely an individual or business is to repay their loans and other debts. In China, the Social Credit System also applies to businesses and individuals, but it is used to measure how trustworthy they are in accordance with following the country's laws and regulations. Given what we already know about China's laws of privacy, Internet rights, and political freedoms, that is one heck of a slippery slope to be living on. Parts of the score are based on an entity's ability to pay bills on time, abide by all laws, and report financial data accurately. Needless to say, Mr. Fan's score must have been pretty low when he vanished, considering he was one of the 50 richest people under 50 at the time of it happening. He likely fell victim to another of the system's odd requirements, that each entity is also judged by the behavior of their business partners. Meaning, if I'm the most upstanding Chinese citizen who ever lived, my fate

[3] Liu, J. (2024). *A CEO went missing. Then his bank got a mysterious bill for $11 million.* [online] CNN. Available at: https://www.cnn.com/2024/09/12/tech/china-bao-fan-missing-mystery-bill-hnk-intl/index.html.

could still be tied to the actions of those I work with. If my business partner is flagged as a political miscreant, I'm likely going down with the ship.

If a Chinese person or entity is found to be in violation, they are put on the "irregularity list." That's one step short of being blacklisted by the government, which means nobody does business with you or really even acknowledges your existence. And of course, anyone who is caught doing either of those things sees their own social credit score take a huge hit as well.

The blacklist is a horrifying process that involves both state and local authorities having the right to put someone on the list. It can take 2-5 years to apply to be removed from a blacklist and successfully do so. On the opposite side of the ledger is the red list, which means someone, their business, or a government entity is viewed as the best of the best in China. Those on the red list are the VIPs of the country, with fast access to loans, capital investment, and approval of investments and other special requests. Among the things that can get people's social credit score to fall are, not kidding, stealing, drunk driving, cheating (on a business partner or a spouse), and jaywalking. While some of these things might seem on the edge of being ridiculous, it's just a different version of what the NSA is doing - using any excuse necessary to collect information on a large body of people for its own purposes, none of which hold much water when you look at them from an objective standpoint.

No matter if you're an American, Chinese, or from another country, the simple fact is that governments will use any excuse to collect data, most often under the pretext of national security. Some of the Patriot Act's mandates were banned in the 2015 US Freedom Act, but considering that operations like PRISM were happening totally out of the knowledge of the general public, it's hard to imagine that the government just shrugged its shoulders and said, "No problem," when it lost some of its authority. Even with those restrictions, the annual transparency report from the Office of the Director of National Intelligence shows that NSA collected telephone data for over 19 million phone numbers in the US between 2018-2023.[4] That leads us to one or two conclusions. Either it is seriously overstepping its legal authority or the NSA believes that the number of potential terrorists in the US at this time is equivalent to the entire population of New York State.

[4] Laperruque, J. (2019). *The History and Future of Mass Metadata Surveillance*. [online] POGO. Available at: https://www.pogo.org/analysis/the-history-and-future-of-mass-metadata-surveillance.

Workplace Surveillance

The general rule of starting a new job is to act like your boss is looking over your shoulder when you're on the clock, which keeps you from getting lured into bad behaviors like surfing the Web, going on social media, using your phone for non-work tasks, setting the lineup of your Fantasy Football team, and watching that hilarious video your best friend sent of the cats who have been trained to meow the main theme to "Star Wars".

Of course, for a large number of employees, you don't have to just act like your boss is looking over your shoulder because they are using surveillance equipment in the form of tracking software, security cameras, and even some webcams, and more. New employees are told this is to track productivity, but it definitely seems to dive a lot deeper than that. Just because you're working in an office paid for by someone else on their equipment doesn't mean that you suddenly give away all your privacy rights. Monitoring in the workplace should be for the purposes of:

- Providing evidence in case of a lawsuit
- Ensuring that all company resources are used properly
- Monitoring employee productivity
- Preventing internal theft of resources, IP, etc.

None of those four have anything to do with reading someone's emails on the server, charting what websites they go to during their break or their lunch hour, or putting an app in their workplace that triggers a webcam to start recording everything they do as soon as they log on to their virtual desktop at 8:01 a.m. What part of the productivity scale is being satiated by seeing what an employee had for lunch or what they are searching for on Amazon as a gift to their daughter for Christmas? Using video surveillance makes sense if your business stores valuable goods, such as in a backroom or a warehouse. Focusing a camera on your employees as they sit in cubicles is going to make them feel like they are doing something wrong, and rapidly expand the rate at which they start looking for a friendlier work environment as well. Other bad choices for companies are to use biometric technology to track time and attendance in place of computerized clock-in/clock-out options. Certainly, the system efficiency is nice, but who wants to give their fingerprints or a scan of their retina willingly to some third party that will store it in a cloud environment somewhere? It's bad enough when we get the letter in the mail saying our password to an app we stopped using six months ago has been stolen; how will we feel when we find out that it's our one-of-a-kind genetic material that is now in the hands of someone on the dark web?

A less harmful and intrusive manner of achieving this is through cloud-based access control, which lets employers see what clients have accessed what files, folders, and tools on a platform. This is a much easier way to maintain control of systems than by tracking everyone. For many companies, the tracking comes before an employee even works for the company! Many places use social media monitoring software (SMM) to check up on potential hires and what their social media accounts say and keep on tracking them while they work there to see if their posts and views reflect negatively on the company.

Financial Surveillance

As privacy goes, people get extra prickly when they learn that someone else is peering into how they spend their money. The modern conveniences of online banking, being able to spend money and pull it from all sorts of sources is a revolution in itself, but just because we like being able to see inside our bank account at any given moment certainly doesn't mean we want a bunch of strangers having the same ability.

Having banks analyze spending and share that information with their customers doesn't seem that intrusive. Most of it is done to help customers track their spending, see where they are applying too much, and try to find ways to be better about staying within their budgets. But knowing that banks are also sharing this information with marketing companies is a horse of a different color. The bank-customer connection is supposed to be a two-way street between our money and the financial service we choose to manage. But the fact that banks are sharing our spending habits with someone else sends all sorts of red flags because it confirms our worst fears that our banks are a lot more about making money than about protecting us. The more information a bank can have about our spending habits, the more it can offer products to use like credit cards, loans, and other accounts to encourage us to put even more of our money into its coffers. Most banks have in their extremely lengthy list of things we have to agree to at the time of signing up for an account that they are often agreed to without being noticed.

With more and more people veering away from traditional banks and into digital wallets like Apple Pay and Google Pay, we are simply adding fuel to the fire. We know from

Part I that these two entities love harvesting our data, and getting it from the first row of the bleacher is even more appealing. These apps on your phone gobble up information in the blink of an eye, using Near Field Communication, Quick Response codes, and Magnetic Secure Transmission that allow your device and the reader in the store you're at to communicate, store payment information, and generate a magnetic signal that is the equivalent of a card swipe. Your purchase data is encrypted, which keeps it from being stolen—theoretically—during the course of the transaction, but it also gives it the perfect home to stay until Apple or Google or whoever comes to collect it and add it to your already bulging file in Google or Apple's cloud. If you ever download Google's totality of your information expecting to see emails and web addresses, you'll be in for a shock when you realize all your purchases from Google Pay are there as well.

Travel Surveillance

We all know the post-9/11 drill by now. Going to the airport without a valid form of ID is like going to the laundromat without quarters. You won't get very far and you'll be really bored for a long time. In the US as another direct consequence of the attacks of 9/11, the process of getting on a plane went from your bag on the X-ray machine to taking off your shoes, pulling out your electronics, and not carrying any liquids over a couple of ounces, showing your ID, removing your glasses, having your children questioned by a stranger, and finally put into another long line.

While you can't fault any country for making sure people are who they say they are, the extra steps can feel unnecessary as we're being asked to have our ID scanned over and over, often being pulled out of line, and asked questions like: Where are you from? Where are you going? How long will you be there? And even pulled out of a line if something doesn't pass the algorithm's smell test and sent to a small room to be questioned by an unpleasant person who keeps reassuring you that it's for our own safety.

Additionally, there are cameras everywhere, with many of them trying to harness anyone committing so-called suspicious behavior, which seems to vary from country to country and even from airport to airport. A man rushing through the terminal to confront his ex-fiancée might be a bad fight waiting to happen that needs security intervention. A man rushing to the bathroom after eating too many chili fries looks the same on camera but definitely has a different meaning. Airports are an ideal place for biometric face recognition devices, as government agencies reason that the fastest way for a bad actor to reach a target destination is by air travel.

What we know about the deficiencies of facial recognition software is only exacerbated at a place of such massive transportation, however. First is the problem of not recognizing people based on different skin tones, which is only amplified in large international airports. Second, is the question of where all of the data that the algorithm is checking facial scans against comes from. Even in a relatively finite space like Detroit, with mug shots and official government ID cards, the police have still botched several cases of misidentification, resulting in wrongful detainment. How could things be anything but worse at an airport, and instead of someone being accused of theft or carjacking, the stakes rise to having to prove you aren't an international terrorist with a reservation for Guantanamo Bay in your future?

Even a trip from a hotel to the airport and onto a plane leaves behind a massive data footprint for most people. Checking out at the hotel puts a charge on your credit card and also means you are on the move towards the next part of your trip. Whether you rent a car or call for a ride, you can be tracked by your own phone or that of the driver; as well as the trackers that Uber and other businesses put on the cars to make sure they know where their staff is. Getting to the airport sees a traveler passing through all sorts of security checkpoints; some obvious, others not so much, with layers of security personnel hiding in plain sight and others where you least expect. Showing your ID repeatedly to at least three different people is required to get on the plane, and any purchases you make while in the airport just add to your profile and your footprint along the way.

All of this information going into one place, whether it's the airport’s own database or passed onto the government of the country you’re currently in has tremendous dangers. There is no way that every airport in every country on Earth can have the same standards of cybersecurity and/or cloud security.

Does an airport in Uganda have the same data privacy and protection plan in place that one in Los Angeles or Abu Dhabi does?

Part 3
Smart Devices and the Internet of Things (IoT)

To the majority of people comfortable living with technology in the 21st century, the quick development of the Internet of Things (IoT) has been more of a novelty and less of a game changer.

Having a refrigerator that can tell you that you need more milk or a thermostat that lets you know that the temperature in the playroom has exceeded 75 degrees is convenient if not exactly earth-shattering. In fact, the first generation of smart devices has been far more of a headache than a gift for everyday people. Of course, the companies that make sensors that go in your fridge, your car, your clothes (yes, really), and every other gadget that used to seem a lot similar wasn't exactly making them convenient just for the consumer, but as a great way to squeeze a whole lot more information out of them for their manufacturers who want to turn customers into data sets to figure out how to maximize their future profitability.

Smart devices and the IoT are two of the very worst examples of something that I like to call the *Jurassic Park* syndrome. In Steven Spielberg's film version of Michael Crichton's remarkable novel, there's a scene inside the resort of the soon-to-fail dinosaur preserve. The character of John Hammond, played by Richard Attenborough, has just introduced his handpicked experts —a paleontologist, a paleobotanist, and a chaotician to his prized brachiosaurus and several other very real, very live dinosaurs, which truly blow their minds, only to then be engaged in a debate about the animal's existence in the modern world, and what it will mean to their fates and that of humanity. In the heart of the discussion, the character of Ian Malcom, played with sardonic aloofness by Jeff Goldblum, puts Hammond on his heels with the moral argument: "Your scientists were so preoccupied with whether they could, they didn't stop to think if they should."

It is a brilliant bit of script writing that could be used to describe most, if not all, of our many digital inventions in the last 25 years, from cell phones and smartphones to social media to wireless everything to drones and remote computer control.

It is perhaps the fundamental problem with the age of digital technology that previous generations didn't have to deal with, as most of their innovations were physical products that had to pass all sorts of rigorous testing and approval to ever even see the inside of a single store. These days, a 10-year-old could code an app, get a free website, or post it on an open-source forum, and launch it into the real world with little to no responsibility for how it is used or what it might actually do. Putting smart sensors into just about every type of household, office, and transportation device to gather more information and ostensibly maximize efficiency might have seemed like a good idea, but doing so without the customer's knowledge or understanding, and for years, doing so without adequate security for the device itself and the data being sent, has had lots of unfortunate consequences and bad results.

The story is nearly a decade old, but the glaring lack of foresight is a perfect example of why devices with smart sensors are such a risk to people who have them in their lives.

The year was 2016 and on a random Friday in October, it suddenly looked like the sky was falling online as the likes of Twitter, Tumblr, PayPal, Pinterest, the BBC, Etsy, Fox News, GitHub, HBO, HostGator, iHeartRadio, Mashable, The New York Times, Reddit, Shopify, Slack, Spotify, Starbucks, and many more all stopped responding to normal web requests. The common thread in all of those companies' Internet presence was Dyn—a private Internet performance management company that acted as a host for multiple major domains. Headquartered in New Hampshire and founded in 2001 by a college student, it had quickly gotten on board in the DNS service industry and was considered an industry leader by the middle of the 2010s.

Beginning around 11 a.m. UTC and lasting for a good 11 hours, Dyn started experiencing massive failures of its DNS offerings, particularly in the major coastal cities of the United States. The attack soon registered as a consecutive distributed denial-of-service (DDoS).

A DDoS can happen organically when a large number of Internet users all try to go to one website at one time, and the number of requests supersedes the bandwidth that the website has for such a thing. We see this occasionally, usually in conjunction with a release of tickets to a sporting event or a concert, like the 2023-2024 Eras tour by Taylor Swift. In the early days of the Internet, DDoS would often occur on college campuses when hundreds or thousands of students all tried to register for their classes online at the same time.

What seemed like some sort of cyber super strike against these websites turned out to be just the opposite. The perpetrators—who were never caught—used hundreds upon hundreds of simple pieces of digital technology to carry out the attack - among them baby monitors and home gateway network devices. If you're wondering how a baby monitor could be used to take down the likes of Twitter and Reddit, it's a pretty clever thing, if it wasn't so scary. Simple devices like baby monitors, routers, refrigerators, and other IoT devices that don't have any sort of traditional input/output functionality come with a default username and password for the Wi-Fi connection that allows them to send their data back to their parent company. When people buy these devices, they are encouraged in the owner's manual to change the ID and password away from the default to practice good cybersecurity. However, you can draw your own conclusions on how many people are following that recommendation, let alone actually reading the advice in the users' manual.

Thus, hundreds of these devices are all broadcasting at the same time using the same username and password. Meaning if a person were to hack said network with the right tools, they could take control of all those devices and change the address to where they were trying to send their data signals.

So, instead of sending user rate information to the maker of the baby monitor every 24 hours, the IoT sensor was instead commandeered to try to reach the same website repeatedly, as many times as it could for as long as it could, over and over and over in conjunction with thousands of other machines conscripted to do the exact same thing. Imagine a sparrow landing on top of a rowboat in the middle of the ocean. Its weight is so light that the people in the rowboat wouldn't even notice the change. But what happens when 100 sparrows land there, and then 500, and then 1,000, and then 10,000? Eventually, it's too much to bear and the rowboat sinks. That's exactly what happened to all of Dyn's websites when they were hit by thousands and thousands of requests in a non-stop fashion; eventually, the server bandwidth buckled under the constraint and the websites went down. All of the people who normally use those websites unwittingly added to the problem by constantly trying to load and reload them, believing the problem was on their end. All those extra requests were denied as well and the problem escalated. Dyn took the brunt of the blame and its stock plummeted. Less than a year later, it was bought by Oracle and ceased to exist.

The purpose of this DDoS attack was sheer mayhem and to show the world how easily such a big part of the Internet could be taken down. A year before in the UK, a DDoS attack was perpetrated by hackers against a business called Carphone Warehouse. The DDoS took the site offline for customers, also using IoT devices to keep pinging the limited bandwidth until it couldn't handle it anymore. But this wasn't just a flex of power, the hackers used the DDoS attack as a distraction, then stole the personal information of 2.4 million customers, the credit card details of another

900,000, and the personal records of 1,000 of the business's staff members[1].

For the business in question, it wasn't just a matter of losing its customers' data and their trust, but a massive hole in their security that cost them dearly. The British Information Commissioner's Office ultimately fined the company the equivalent of $500,000 after an audit showed that the company's approach to data protection was sub-par. Since those early days of one debacle after another, brands all over the world have had to go back to the drawing board. They've reworked how they build IoT and how they monitor edge computing. More importantly, they've had to make the sensors a lot less flimsy, incorporating security features that can take a lick from a dedicated cybercriminal and keep on functioning. The EU's Cyber Resilience Act was a landmark regulation that demanded more out of sensor manufacturers and companies were charged with lowering the latency time—the distance in both time and geography that a signal has to travel from its source to its destination, which lowers the chances of it being intercepted.

If life were a horror movie, Amazon's Alexa, Apple's Siri, and Google Home would be the surefire villains that everyone's afraid to be alone with. It's the sort of invention that anyone who has ever seen or read "2001: A Space Odyssey," read "I, Robot" or watched the more recent version of "Battlestar Galactica" will always point to when

[1] Global Relay Intelligence & Practice. (2023). *Green light for legal action over UK's biggest data breach.* [online] Available at: https://www.grip.globalrelay.com/green-light-for-legal-action-over-uks-biggest-data-breach/ [Accessed 20 Nov. 2024].

we talk about life imitating art. Here is a machine—so tiny it could fit in your pocket or your purse—that can imitate human speech, listen to everything we are saying, is connected to the Internet 24 hours a day. It records our voices and our speech in order to get a better idea of who we are, what we like, what we buy, and so forth, and not a single one of us knows just how sophisticated it is, what its limits are, or how much information of ours it is understanding and passing onto its makers.

Let's think about that from an objective standpoint and try to figure out how we got to this level of comfort with a machine we know next to nothing about.

Here's the hypothetical: A stranger approaches you from a company and wants to put this little round machine in your home. It plugs in and mostly just sits there, glowing from time to time. Here's what he tells you about the machine:

1. It's going to learn to distinguish your voice from everyone else's and eventually call you by your name—without you giving it permission to.
2. It's going to make suggestions of things you might want to buy, even though you never ask it to do so.
3. Sometimes it won't seem to hear what you're saying, even though you're standing right next to it. When this happens, you will get more and more angry and talk to it louder and louder like it has some sort of hearing problem.
4. Sometimes it will start talking based on something you said, even though you did not address the machine at all.
5. Sometimes it will flash content or give suggestions based on something you queried on another

device, even if you weren't at home at the time you made the query.

6. It will sometimes refer to itself as a living entity, but when you ask it more specific questions on how it was made or what is inside of it, it will give childish, humorous answers instead.
7. It will only tell you that it can't do things, but not the reason why it can't.
8. It is constantly receiving updates, but not telling you what those updates are
9. It is constantly sending information back to its maker about you and your family, again without telling you what is being sent.

What do all of those facts make you think of?

For a lot of people, it sounds like a machine meant to spy on you and be purposely vague or downright opaque when you ask questions about the machine or its purpose. Now clearly, we're moving the goalposts a little with the above description.

Siri, Google Home, and Alexa are also dynamite with answering simple questions, playing music, setting timers, telling you the weather, and plenty of other functions that can be very handy and very helpful. The problem though is that we are not very sure that the things that it can do balance out the things we don't know about it or don't like about it. Let's break down some of the facts and myths about our virtual assistants who have become so commonplace in homes, offices, hotels, and more despite how very little we know about them.

The device is always listening for its "wake word", which is typically its name "Alexa," or "Hey Siri". Once it hears that, the machine starts recording your voice and when you are done talking, it sends your request to its cloud server to be processed. This takes place in a very short amount of time—analyzing your speech, using algorithms to figure out what you mean, and then sending back a response. Manufacturers claim these devices only record speech directed at it, but anyone who has ever owned one can certainly recall at least one time when the device will start talking in the middle of a conversation or ask you to give a better explanation of what you're asking, even when you aren't asking. The machines are supposed to erase your conversation as soon as the request is confirmed, but can also be stored locally or in the cloud in order to improve the machine's efficiency in understanding your requests and being able to respond to them more quickly.

But what if we want privacy in those conversations?

What if you ask Alexa how to stop drinking or ask Siri what the phone number for the National Hotline Prevention network is? It is unlikely anyone would want the virtual assistant blaring that information back to data analysts at Google or Apple. Even less likely they'd want the information stored long term where it could be hacked and used against them.

The Truth About Virtual Assistants

The biggest mistake that anyone can make when using Siri, Alexa, or the other virtual assistants out there is assuming your conversation is in a closed loop. You might not see it happening, but the moment you speak, whatever you've said is being sent to the parent company for analysis. And since those companies are still run by actual human beings, that means that you don't have the privacy you think you do. Nor is it just Amazon or just Apple or just Google who is privy to all your requests.

These big companies have stacked partnerships to offer services via the virtual assistant, like Amazon Music, Audible, your local grocery store, or ESPN. Those companies don't just offer their services to Alexa or Siri for money; they do it for a big slice of the data pie that you're serving up daily with your requests. This means that your requests—from the mundane to the potentially embarrassing ones—aren't just winding up in some random Google or Amazon file. Instead, they are heading to a variety of different companies with its own agendas for using your data. The worst part is that with one sweeping swipe of your finger or pressing of the "OK" button when you set up the device, you agreed to ALL of the data parsing, analysis, and marketing for all of those companies. So, when ESPN sees that you asked to check the score of a college football team that most people have never heard of 150 times over a two-hour period, their algorithm is probably thinking you went to the school and would like to have a bunch of advertising for the school's merchandise sent to you, or you're a degenerate gambler who would love a whole slew of gambling site invites sent your way.

When you tell Alexa to play you some “bedroom music” to celebrate your one-year anniversary with your wife, well Amazon Music relays that message back to Amazon itself who decides you might be interested in some more adult-themed products placed on your “other customers bought this” list. The device might fool you by learning your first name and remembering your favorite things, but it is not your friend. Its sole purpose is to gather as much information about your tendencies in order to insert the parent company’s ability to advertise to you and to sell your data to its partners. It’s almost a form of willing wiretapping, where you can imagine the police or government agent listening to your conversations with one ear while typing out their file on you from a secret location.

That’s also not too far from the truth in some circumstances. While the voice assistant is entirely AI, there are employees of each company further up the line that manage how those AI systems interact with humans to ensure that it is functioning to their standards.

Human reviewers are hired by all virtual assistant companies as somewhat of the last line of defense and review, listening to anonymous conversations and transcribing the recording to see how the app is doing. But since we know that the devices are sometimes recording conversations not meant for their ‘ears’, what happens when a human listens to one about someone confessing to a crime or contemplating suicide? Is it just all more data with no moral recompense?

That question has been answered several times in the past decade with people accused of various crimes having “their” personal devices used against them in a court of law.

From 2014-2018, there were at least 6 instances of Amazon and other big brands turning over recordings from devices in the homes of people accused of murder as evidence.

The glaring red flag here is this: If the companies tell users that the machine immediately forgets what they say after they say it, then how are police able to listen to recordings made weeks, months, or even years ago?

As it turns out, you actually have to change the settings on the device to make it stop saving recordings. And you'll never guess what the default setting is. That's right, never.[2]

If you don't change those settings, the device will record and save everything you say forever. If you do go into the settings, the only options for saving messages are: three months, 18 months, and forever. If you want to delete what you've said today, yesterday, or last week, you have to go onto the settings on the screen or your app and do it there, or tell Alexa to do it. Although then there's a record of you saying to delete them!

In 2018, a New Hampshire judge compelled Amazon to turn over recordings from a double murder of two women by a friend and acquaintance. Amazon refused until the request became a legal order, then complied. The man, Timothy Verrill, was later convicted of both killings and sentenced to more than 100 years in prison[3].

[2] PCMAG. (n.d.). *How to Review and Delete Your Alexa History*. [online] Available at: https://www.pcmag.com/how-to/review-and-delete-your-alexa-history.

[3] News, A.B.C. (n.d.). *Judge orders Amazon to hand over Echo recordings in double murder case*. [online] ABC News. Available at: https://abcnews.go.com/US/judge-orders-amazon-hand-echo-recordings-double-murder/story?id=59100572.

The concerns about the parent company listening to any IoT device in your home are magnified by who else could be using the device on you. For starters, your assistant is running on the same Wi-Fi that the rest of your home is, so anyone with knowledge of your password and a few simple tools could access the device and start pulling whatever it is uploading and downloading without much fuss.

A little more skill with hacking could have someone eavesdrop on all of your conversations and control any smart home devices you have connected. Someone having the ability to turn your reading lamp on and off might seem like the greatest mastermind criminal of our time, but what if they are also turning your thermostat to its lowest setting on the hottest day of the year or vice versa on the coldest and running up your power or gas bill? What if you have a Ring system attached that lets them view every room you have a camera in? Now they can spy on your family members, know when you are not at home, and make a pretty good map of your house and where the valuables are. Combine that with a Smart Lock and they can be in and out of your house without you even realizing they were there, despite all of that glorious technology on hand.

In the early days of the nanny cam, there were stories every month of people believing they were being spied upon, including a Minnesota family who found hundreds of photos of their nursery online and a Texas family who reported a hacker was calling their 2-year-old daughter explicit names after gaining control of the system.[4]

[4] ABC30 Fresno. (2015). *Minnesota family's nanny cam hacked from overseas*. [online] Available at: https://abc30.com/nanny-cam-hackers-hacked-hack/634416/.

It's not just the assistants that are double-dipping on our data, but also Smart TVs and other appliances. People in the know claim that Smart TVs are "pre-hacked", meaning there is already a slew of apps and vendors on its system that will start getting data packages the moment you turn the TV on[5]. Much like Microsoft Windows stuffing each new version full of apps that you can only avoid, not delete, Smart TVs are hardwired so you can't stop them from sending data. The only thing that mitigates what they collect is by turning off the Automatic Content Recognition function, which means it won't track what shows you are watching. Even with that knob toggled, your TV is still watching you just as much as you're watching it.

The aforementioned are all disturbing examples of how invasive technology can be in the home, so what does it look like when you're in public? Perhaps the scariest thing about public Internet is that we all get the same warning every time we log onto it in a public space, a hotel, an airport, or any other network that isn't a direct contract between ourselves and our Internet Service Provider, we read the very specific warning, and don't seem to care.

By law, providers of this kind must display the warning: *This is an unencrypted network, and any information you send or receive may be viewed by others.* After that, we're given the option to either connect or cancel. Of course, we always pick connect, because we're desperate to get online at that point, aren't we? This might be the crux of the entire

[5] ZDNET. (n.d.). *Your smart TV is snooping on you. Here's how to limit the personal data it gathers*. [online] Available at: https://www.zdnet.com/home-and-office/home-entertainment/your-smart-tv-is-snooping-on-you-heres-how-to-limit-the-personal-data-it-gathers/.

argument: We don't really care about the risks of how we're connecting to the Internet as long as we can actually get on the Internet.

Ultimately, a large portion of the Internet-using population is willing to take all the risks of the consequences of what could happen to our data, our devices, etc., as long as we can keep using them.

Take away the technology aspect of it, and what does that sort of behavior sound like? An addiction.

Smokers keep smoking even though their risks of lung cancer are off the charts. Alcoholics don't stop drinking even though they have huge risks of liver problems and legal issues like DWIs. Drug addicts will do almost anything to get their next fix, even if it means breaking the law, losing relationships, jobs, etc. Ignoring the warning signs of Internet addiction might not be as personally harmful, but leaving all our devices open to being spied on and listened to can have tremendously damaging effects on our financial health, our credit scores, our privacy, and so forth.

We even allow ourselves to be dazzled by technology that spies on us.

Part 4
The Dark Side of Convenience

Just like there are two sides to every story, there are often two belief systems as well. While one opinion is to generally trust everyone and believe people have good intentions, the other might say that while that's OK for people, once we're on the radar of organizations full of people with agendas fueled by money, power, and control, the good of the average person tends to go out the window.

A fine case in point of this is the booming hobby of family tree mapping made popular by websites like "23andMe" and "Ancestry.com" as well as TV programs like "Finding Your Roots". Being able to access vast stores of public information—some of it centuries old—has become a massive, consuming hobby for thousands of people around the world. They eagerly jump at the chance to scour old records, scroll through crinkly pictures, and meet with other people in online message boards as they try to piece together their own family trees while helping as many other people along the way as they can. The hobbyist part of this endeavor is truly some of the best of humanity—people going out of their way to help each other get connected to those who came before them with no more interest than a curious puzzle and a kind heart. If only everyone felt that way.

The main two powers in this field originally sold data to many companies, among them P&G Beauty, Pepto-Bismol, the University of Chicago Medical Department, and Glaxo-SmithKline. After being taken to task for this, the companies stopped selling data, a feather in their cap considering what a high price one could fetch for selling not only one person's personal records but access to every person who is related to the original individual. Like the biometric imagery of people's fingerprints and retinas, giving companies access to an individual's highly unique DNA, along with all the personal information that goes with it, feels like the ultimate risk to take when willingly handing over data to a company that is not keeping it strictly inside its own data storage.

Moreover, these companies seem to have no problem breaking their own privacy vows when it comes to dealing with law enforcement, insurance companies, and people seeking to figure out who their parents are if they are adopted or were conceived by means other than a normal pregnancy.

These tests have also been known to shatter families who, for their own valid reasons, kept their children's parentage a secret.

A famous case occurred in 2016 when the websites were really starting to take off.[1] A woman named Michelle, who

[1] Elle Hunt (2018). *'Your father's not your father': when DNA tests*

chose to keep her last name private for the article that appeared in The Guardian, had taken the test along with her husband as a new hobby. Michelle had traced her father's family all the way back to the 1600s and had been saving enough to take the DNA test. She knew there was some Native American blood on his side, and had the wild hair that if that percentage was enough, she might be able to qualify for some college scholarships. Like clockwork, about six months after she filled a vial with her saliva, sealed it, and sent it off to be analyzed, she got the results back, with a very bizarre outcome:

The pie chart that shows where a person's ancestors are from was 50% Italian—but Michelle had no Italians in her family. Figuring it was a mistake, she joked about it but her husband showed her that all the other ancestors matched up on her mother's side of the family.

Suddenly, Michelle was starting to not like where her thoughts were headed. Michelle and her mother were estranged, but she broke the silence to ask about the test, which showed she had a first cousin in Syracuse, NY, with an Italian last name she had never heard of. Her mother denied that the test was accurate, so she called her aunt the next day, told her what she had found, and listened in stunned silence as her aunt recollected that her mother's prom date had the same last name. Her mother denied the facts again and mentioned that her prom date had recently died. Michelle found his obituary online, and it was like looking into a mirror. With her mother still in denial, she

reveal more than you bargained for. [online] the Guardian. Available at: https://www.theguardian.com/lifeandstyle/2018/sep/18/your-fathers-not-your-father-when-dna-tests-reveal-more-than-you-bargained-for.

asked the man she thought was her father to take a paternity test. They had grown apart, and found out the same day in the same way that they weren't related at all. Her mom had lied to both of them.

While this might seem like a bit of an extreme case, the presence of DNA in someone else's database and storage facilities rears its head in other ugly ways as well. Both Ancestry and 23andMe are known to give access to law enforcement on occasion to try and solve current crimes and cold cases as well. Sometimes they have a suspect with DNA but aren't able to make a perfect match, so they see who else has similar DNA and often come up with a win.

Ancestry boasts on its website that it doesn't give out data "voluntarily" and that law enforcement has to "Follow a valid legal process to acquire it."[2] That might sound like tough talk, but it really isn't. It's simply Ancestry saying that if the police want to look at their proprietary information, they have to have a warrant for it. That is no different than police needing a warrant to search someone's home or business. If they have cause, a judge will sign the warrant, and they'll get what they came for. That's it.

A bigger problem comes with the fact that DNA isn't any more foolproof for some cases than anything else. While some cases are full of fantastic results, such as the conviction of Joseph James DeAngleo Jr., who committed at least 13 murders, 51 rapes, and 120 burglaries in California between 1974 and 1986. The genealogy service GEDmatch was able to supply law enforcement with DNA

[2] www.ancestry.com. (n.d.). *Privacy Statement - Ancestry.com.* [online] Available at: https://www.ancestry.com/c/legal/privacystatement.

evidence that connected semen found from a rape kit to the killer's DNA profile.

But the flip side of that sort of climactic ending is the sort of thing that ties back to our first story out of Detroit in Part I of this book: When Big Brother technology goes after an innocent person[3].

In 2014, a filmmaker named Michael Usry was at his parents' house in New Orleans, Louisiana, when he got a call from the local police department saying they wanted to check out his vehicle, as it had been tied to a car used in a hit-and-run. With nothing to hide and full knowledge that it wasn't his car, Usry willingly drove to the station to help out with whatever he could. But the cops hadn't been honest with him. They really wanted to talk to him about a rape and murder that had happened 18 years earlier. He fit the profile of the suspected killer of the woman who had been killed in Idaho Falls, Idaho on the other side of the country. He had passed through the small town twice during the time she was killed in 1996. The cops had gotten interested in Usry because 16 years earlier his father had been part of a DNA swab project that had been encouraged by the Mormon Church.

The police ran the semen found in the woman's rape/murder case, and one of the samples came back as about a 97% match—Usry's dad. Since the older Usry was far too old to have committed the crime, he was ruled out. But using a genetics website, investigators turned their focus

[3] Akpan, N. (2019). *Genetic genealogy can help solve cold cases. It can also accuse the wrong person.* [online] PBS NewsHour. Available at: https://www.pbs.org/newshour/science/genetic-genealogy-can-help-solve-cold-cases-it-can-also-accuse-the-wrong-person.

to the younger Usry, a filmmaker who had previously made a movie about a murdered young girl. Back in New Orleans, the police detained him for two hours and then showed him the court order they had obtained to swab his cheek for a DNA sample. He complied and spent the next month worrying himself to death. A month later his phone rang. It was the police lieutenant. He was told he had been ruled out as a suspect in the case. That was all. No explanation. No "Sorry we scared you to death for a month".

Health Data Exploitation

There is no data more protected in the US than healthcare information, thanks to the laws put down by HIPAA. But since a lot of apps out there are tasked with making these processes go quicker and easier, there are often shortcuts that end up with dangerous consequences. Mental health apps in particular have a real problem with their data. They are ostensibly used for good purposes, like giving people struggling with issues the opportunity to journal their feelings, reach out for help, or do other activities that can refocus their minds.

However, many of these apps don't have adequate cybersecurity, and some of them go as far as to sell client information to third-party companies who want to delve further into this niche and use it to decide what products and services to target people suffering from real-life issues[4]. This became a major issue in 2020 and immediately afterwards as many people battling mental health issues suddenly found themselves unable to see a therapist in person because of COVID-19-related lockdowns. Being stuck in one place as most jobs ground to a halt was also a strain on people's well-being, and many turned to the Internet for stopgap solutions to hold onto their sanity in troubled times.

A study of 32 mental health apps in 2023 found that 22 of them sported a "privacy not included" label, essentially telling customers that they had no guarantees of their information staying on the app. Just as a niche of health, mental

[4] Brookings. (n.d.). *Why mental health apps need to take privacy more seriously*. [online] Available at: https://www.brookings.edu/articles/why-mental-health-apps-need-to-take-privacy-more-seriously/.

health has so many pieces of data that most people would not be comfortable having others find out about—everything from sexual orientation to substance abuse to their most troubling problems. Not only are these healthcare apps being frivolous with the data, but they are also selling it on the side to the highest bidders.

Email and Communication Monitoring

How's this for an impossible choice?

You either forgo the built-in anti-spam protection that a web service like Gmail provides or you put up with Gmail monitoring all of your personal communications. Not much of a choice at all, is there? Either you're bombarded by spam, or you've got Big Brother looming over your desk as you write all of your personal correspondence.

Knocking out potentially dangerous spam emails has been part of the fight ever since email became a thing. Google and Yahoo changed their rules of engagement in February 2024, demanding that mass email senders would have to follow some very strict parameters in order to have their letters delivered. These included having a spam complaint rate of less than 0.3% (no more than 3 spam reports per 1,000 messages) as well as giving recipients the chance to hit a one-click "unsubscribe" button that would do just that within 48 hours.

Despite this crackdown, Yahoo at least continues to do deep scans on individual emails. The company says that its purpose is to eradicate all forms of spam, but criticism still persists that the company is also targeting advertising to the individual based on the content it scans, as well as making data breaches that much easier.

The fact that so many people are still using Yahoo for email is wholly remarkable in and of itself. Its number of monthly users is 225 million worldwide. Trusting Yahoo to protect any information at all is a perfect reminder that people will put up with anything for convenience's sake rather than go with another option that helps keep them and their data safe.

The original powerhouse search engine before Google came striding onto the landscape like some great colossus, at one point Yahoo was getting 2 billion search queries per month around 2002, with an all-time stock high price of $118.75 per share in 2000.

After Google raced past it, the forlorn search engine company started looking for a buyer and began negotiating a sticker price with wireless powerhouse Verizon. In 2016, it was revealed that 200 million Yahoo passwords had been stolen at some point and were now for sale on the Dark Web. The Dark Web—an unmapped, off-the-grid corner of the Internet—is a marketplace for the illegal. A place where people connect to buy drugs, guns, and the very data breaches this book warns about.

A few months later in 2016, Yahoo announced that it believed the message hack was "state-sponsored" and that the actual number of stolen passwords was revised upwards from 200 million to 500 million. During this time frame, Verizon and Yahoo were working out the final kinks of a $4.8 billion deal when the telecommunications company put a hold on the deal.

Running its own due diligence background check into the alleged hack, Verizon found two very interesting facts. The first was that Yahoo had known about the breach since at least 2013 and didn't bother telling anyone, including the affected users, for three years. The second was that it wasn't 500 million users affected; it was every single Yahoo user. All 3 billion of them at the time. Yahoo's staggering lies of omission cost the company $350 million as Verizon dictated the new selling arrangement.

Yet somehow, almost a decade later, 225 million people are still trusting Yahoo to take care of their email accounts?

Part 5
Real-World Consequences of Privacy Erosion

We've danced back and forth between hypothetical worries and real-life debacles that happen as a result of the overbearing surveillance decisions being made by governments, corporations, social media platforms, apps, and digital technology companies. We keep seeing different versions of the same threats, the same disappointing tendency by those in power to favor power and money over freedom and fair acts, and the slow decline of liberty replaced by the consolidation of power. The failing of basic freedoms as tech companies turns everything into a data race is not something that will happen all at once, but through a process we call privacy erosion.

When rain and wind wear away at the sand on a beach or the face of a cliff, the effect is not immediate, and maybe not even noticeable at first. Only after considerable time can one begin to notice a difference in the way the geographic feature looks, and only considerably more time from there before the beach is unrecognizable or the cliff collapses on itself.

We are in the process of seeing this exact same sequence take place as our freedoms are becoming eroded with the weight of giant companies wanting more, and big-time government departments having no problem playing fast and loose with the laws of the land in order to get their desired goals achieved. In this part, we're going to take a closer look at some key events over the past decade or so in which the singular focus on surveillance and data acquisition has gone very poorly for the parties involved.

The Strava Heat Map Military Debacle

Two things are universally true of life in the American military. #1 - You're going to be in the best shape of your life. #2 - There are likely going to be times when you are somewhere that you can't officially say you are.

As regards the first statement, the US military equips its personnel with fitness apps and hardware in order to give each person their own opportunity to track their fitness, but also to track soldiers' performances as a whole to see what recommendations are working and which are not.

One such app is Strava. Based in San Francisco, Strava uses a smartphone's GPS to track the exercise activity for each user's activity route. As of January 2018, there were 27 million users around the world. In an effort to drum up business with a little visual data art, Strava offered heat maps to individual users that function somewhat as a piece of artwork, showing each customer what their exercise tendencies look like. Perhaps seeking to draw some social media coverage, a few virtual videos, and so forth. The map showed the whole world of Strava fitness routes, overlapping and appearing in the middle of nowhere in some cases.

The last heatmap the app put out showed aggregate data from 2015-2017, with more than 17 billion miles covered and more than 1 billion total activities achieved. A 20-year-old Australian college student unspooled some unspoken conclusions while examining the map on a cartography blog[1]. The student realized that the high number of soldiers

[1] BBC (2018). Fitness app Strava lights up staff at military bases. *BBC News*. [online] 29 Jan. Available at: https://www.bbc.com/news/technology-42853072.

on bases doing frequent activity was illuminating patterns that made the bases themselves, some of their assets, and the precise troop movements very easy to see. From the above satellite map, entire layouts of bases were revealed, including what looked like obvious American and Russian missile silos, given the number of times that activities involved running around large, cylindrical spaces.

Even more damning was the fact that it appeared there were American bases in many areas where no bases are officially believed to exist. Since the US military is known to have a deal with Strava and it seems highly unlikely that the local populations of rural areas of Syria, Iraq, and Afghanistan all decided to get in shape and buy American-made fitness apps.

Strava's map had done something that would get a military member court-martialed—exposed previously classified American military positions.

Multiple unidentified airstrips being used as jogging tracks in places where neither the US Army nor the CIA has a presence in Afghanistan topped the list of curious spots. Not only are the bases illuminated, but so are the roads connecting them, which experts say could easily be used to sabotage American troops. Further analysis reported by The Daily Beast and conducted by Dr. Jeffrey Lewis of the Middlebury Institute showed the likely location of a secret Taiwanese underground missile command complex, that would shield the country's president during a war, and is likely the tiny country's most important base against any potential military action from nearby China and North Korea.

Ring Doorbell Cameras and Law Enforcement

Ring cameras are everywhere and seemingly capable of capturing everything. People have them on the outside of their homes to protect against prowlers in the nighttime and solicitors during the day. They are great for warding off package thieves and making sure the kids are safely in bed as well. In recent years, however, Ring footage has made its way more and more in the news for being released to both law enforcement and the general public without the permission of the person whose camera it is. Plenty of times, the owner of the camera volunteers the footage if they know something nefarious has taken place within sight of their exterior cameras, but in other cases, there appears to be a clear-cut conflict of interest about how and why the Ring footage, ostensibly the property of the person who has bought the equipment from the company—is accessed and shared without their consent.

An interesting case concerning this very issue broke news on the entertainment network TMZ in November 2024. Jaxon Hayes, a member of the Los Angeles Lakers, was being investigated by the National Basketball Association after Ring footage appeared of him at his home in 2021 having a lengthy argument with his then-girlfriend. In the video, Hayes appears to push the woman out of the way when the two cross paths in his driveway, and he may have spit on her as well. In other parts of the video, the woman is heard yelling at him to stop and that he is hurting her, but no corresponding video evidence can be seen.

All of this video came to light more than three years after the incident and what followed it. Hayes' girlfriend called police, who intervened at the same home shown in the Ring footage. The body camera used by the police showed Hayes shoved the police officer and then got tased and arrested. Initially met with 12 charges, he wound up pleading no contest to two minor charges and received three years' probation and 450 hours of community service. At the time, Hayes was in his second year with the Pelicans after being their first-round draft pick in 2019. The NBA investigated the incident initially and did not punish Hayes. The first off-season after his trial, Hayes was released from the Pelicans and wound up signing with the Lakers.

Earlier in 2024, the woman he allegedly assaulted, filed a lawsuit against Hayes. A few months later, the mysterious footage showed up, despite it being Hayes' house and presumably his Ring camera. Perhaps spurred on by Hayes' case and others, in January 2024, Ring backtracked significantly on its position, announcing it would no longer abide by requests from police for footage without a proper warrant[2]. The announcement came after years of protest and backlash from the public.

Earlier in its tenure, Ring let officers either directly send a request for footage to the user's email address or publicly post requests on the company's Neighbors app. Now the officials have to proceed with a warrant request to get access.

[2] Guariglia, M. (2024). *Victory! Ring Announces It Will No Longer Facilitate Police Requests for Footage from Users*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2024/01/ring-announces-it-will-no-longer-facilitate-police-requests-footage-users.

Telecom and ISP Data Collection

We all know that the various telecommunication companies will go to great lengths to get your business. Free channels, free smartphones, lowered bills, the whole nine yards. But in 2021, it was revealed that based on how much money these companies were making off scraping consumer data and selling it to advertisers, the jig was up. A report by the FTC broke down the privacy practices of six different ISPs and their advertisers that showed that the companies were bathing in data including browsing history, behavioral data and location. The big companies were then selling that data right to middlemen who turned around and cashed in on selling it to advertisers.

"Even though several of the ISPs promise not to sell consumers' personal data, they allow it to be used, transferred, and monetized by others and hide disclosures about such practices in the fine print of their privacy policies," came the damning statement by the FTC. "Many of the ISPs also claim to offer consumers choices about how their data is used and allow them to access such data," the FTC said. "We found, however, that many of these companies often make it difficult for consumers to exercise such choices and sometimes even nudge them to share even more information."

Perhaps the worst part about the ISPs' behavior is how brazen they are about selling the data. It's the same sort of ego we saw from foreclosed bank executives at the start of the Great Recession. As detailed by then-President Barack Obama in his book A Promised Land, the C-suite executives of these giant banks were still planning to use the government's bailout money to pay their full salaries and award themselves large Christmas bonuses, even in the face of financial ruin.

The ISP providers went hog wild on collecting and selling data because they simply didn't think life would ever change.

Part 6
Protecting Yourself in a Privacy-Invaded World

If you want to lose weight and keep it off forever, you can't just follow some 10-step program you found on a blog to do it. If you wanted to get in the best shape of your life, you couldn't join a gym for a month and figure that the muscle you put on in those 30 days would last a lifetime. There are no short-term solutions for comprehensive changes, and protecting yourself and maintaining as much privacy as possible when using the Internet is as fundamental a change as most people will have to go through to achieve the level of safety that everyone should strive for. The system is extremely flawed in its current incarnation. You can't rely on corporations or service providers or even the government to help you fix the immediate problem of how little protection you currently have. We'll talk about the way to fight that sort of gross lack of oversight in the next section.

Want to protect yourself in a privacy-invaded world? You have to start living counter to just about every instinct that the convenience of Internet use has built into your stems and in a different way than most people you know.

If you want to stop gaining weight and get healthy, you'll stop eating processed foods, sugars and eating after 5 p.m.—pretty much counterculture to every single person you know. If you want to retire debt-free, you'll change your spending habits so that you're never buying anything on a credit card that you can't afford to pay off the same month, even though that might mean saving for years for a vacation or a car, or anything else that most people charge and forget about.

It all comes down to what you are willing to risk and what is important to protect with online privacy. It will take a powerful effort from all sides of the argument in order to get companies to stop making decisions that poorly affect consumers, as well as the desire by customers to stop using popular apps in order to get the severity of the point across. In the meantime, the onus of protection falls to the individual Internet user.

It starts with understanding what you're signing up for in every relationship you have with an ISP, a SaaS, an app, your phone, and any IoT device that you happen to purchase or use. Don't scroll all the way to the end of the terms of use and swipe OK just to hurry that process along. That's tantamount to agreeing to an employment contract without reading a single word or accepting the judgment from a civil court by signing the last page without considering what is written on the previous ones. It's foolish and short-sighted, and all you're telling the other party is, "I don't care about my own protection". Yet we do it in almost every circumstance.

An app could include the phrase, "By signing this, the customer agrees to name the company sole heir to all their funds in their will", and most customers would never be any the wiser about what they had done. Reading the terms of use is a lot like voting. If you don't participate, you have no room to complain. So, when you agree to terms as fast as possible to get some new addictive game on your phone, then suddenly start getting a slew of texts from the son of the deposed King of Nigeria asking for help to transfer funds to a bank account, you've done that to yourself.

A big part of staying private is staying silent online—both literally and figuratively. We all have social media profiles, old websites, and old emails we don't use anymore, or have forgotten that we ever had. Each reference to ourselves online is one more that lets all sorts of web creatures crawl over our ID, whatever personal information we have, and anything else we've parked online without realizing at the time how bad of an idea that was. Anyone under the age of 35 or so has grown up with the Internet as a constant part of their lives, and as bad as adults are at leaving their information in easy-to-find locations online, kids are even worse.

Not only do studies across the board find that increasing use of screens and social media is bad for kids as they develop, but they also 'overshare' personal information through pictures and posts.[1] Removing all old references to yourself, including anything that includes any personal information —past or present—is a must. Literally silencing yourself

[1] Jiang, K. (2023). *'Overwhelming' evidence social media is linked to bad habits in children from gambling to drug use, new study finds*. [online] Toronto Star. Available at: https://www.thestar.com/news/canada/overwhelming-evidence-social-media-is-linked-to-bad-habits-in-children-from-gambling-to-drug/article_47ff6530-937c-11ee-921d-17f88c3dfa3f.html.

means turning off all microphones on your IoT devices when you aren't specifically talking to them.

Siri's job isn't to listen to everything you're saying and decide when to chime in, but to respond to your voice commands, and only your voice commands, directed specifically at Siri.

Science fiction has become fiction more than a few times in this regard. In 2018, a couple in Portland Oregon witnessed its Alexa secretly recorded a conversation they had without invoking the device's name and sent it to an employee of the husband who appeared on their contact list. [2]

The family had devices in every room and the employee was sent the conversation that had been recorded, then called the couple to tell them that they should unplug all their devices because they were either being spied on or had been hacked. They didn't believe him at first until he started telling them details of their conversations, such as talking about getting new hardwood floors. When interviewed by a local TV station, the woman described their call to the Alexa helpline. They said, 'our engineers went through your logs, and we're sorry'. He apologized like 15 times in a matter of 30 minutes, and he said we really appreciate you bringing this to our attention."

When pressed for details by the TV station, Amazon offered a reason that, on the surface, seems a bit far-fetched.

"Amazon takes privacy very seriously. We investigated what

[2] Horcher, G. (2018). *Woman says her Amazon device recorded private conversation, sent it out to random contact*. [online] KIRO. Available at: https://www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private-conversation-sent-it-out-to-random-contact/755507974/.

happened and determined this was an extremely rare occurrence. We are taking steps to avoid this from happening in the future. Echo woke up due to a word in the background conversation sounding like 'Alexa.' The subsequent conversation was heard as a 'send message' request. Alexa said out loud 'To whom?' At which point the background conversation was further misinterpreted as a name in the customer's contact list.

Alexa then interpreted background conversation as 'right.' As unlikely as this string of events is, we are evaluating options to make this case even less likely."

The end result was good for the client because there was a good Samaritan at the other end of the technology. But what about the cases when that doesn't happen? And how could such a carefully trained algorithm make so many seemingly unlikely mistakes in a row to come to the conclusion that all that private information that it shouldn't have heard in the first place should be sent to someone on their contact list? Very suspicious.

Moving on to your online life, we've all been in the spot where we do a search for a product one day, and then every site we head to afterward has plugged-in ads for that same product or one like it. Not too terrible when you're researching cars, but what about when you're looking for a good pregnancy test or hair replacement system? None of us should be followed around by the things we're looking for online.

If I take a look at hunting rifles at the sporting goods department at Walmart, a salesman isn't going to follow me into the baby clothes section asking if I've thought any more about that hunting rifle. But online tracking is exactly like the default deal you get when you are lazy in how you accept terms for your Alexa, your Smart TV, the app that lets you control your thermostat from 1,000 miles away, and everything else that is connected to a Big Brother somewhere. If you just accept what the manufacturer wants instead of taking your rights into your own hands, you have nothing to complain about when your information gets sold to every Internet ad company out there.

So, start protecting yourself by going into your operating system—whether that's Windows or macOS and opting out of the targeted ads. That's how advertisers are able to start a file for you, by using a number assigned to your Microsoft or Apple ID so they can track you regardless of what device you're using or where you are. Pretty insidious, right?

Or if you don't trust either major operating system to protect you, consider switching entirely to a Linux system. Linux has been around for more than three decades, but remains quite popular—it powers the Android system in fact. Not only is Linux an open-source, free system to start using, but it also is incredibly reliable against all types of malwares, unauthorized access, and breaches of the vital data that your computer system holds. Using Linux requires learning a new way of doing things, but most people pick it up quite readily, and isn't your online security worth a little extra on-the-job training?

Before you get back to surfing online, you need to sign up for a virtual private network (VPN). A VPN is a secure connection that allows you to send and receive information from the Internet or a privately owned network. It uses an encryption process to make it impossible for anyone to see what data is moving to or from your computer. It works as an extra layer of privacy and security for your online activity, especially when using unsecured networks. VPNs aren't just for individuals using the Internet in public. Companies also use them to move secure data across the Internet to ensure a secure transfer between networks.

Once upon a time, the Internet was referred to as the 'information superhighway.' We can use a visual analogy to describe how a VPN works. Envision a highway full of cars representing Internet users. From above, we can get a lot of information about them—what color car they have, how fast they are driving, what exit they are getting off at, their car model and age. And if we look closer, even their gender, the number of people in the car, etc. Now imagine that instead of a highway, it's a covered tunnel, like the kind that cuts through mountains or goes underwater between destinations.

From the outsider's perspective, we are still certain there are cars passing through the tunnel, but their identifying information—color, model, who's driving, etc.—is hidden from our view. A VPN serves as your covered tunnel. It establishes an encrypted connection between your device and a VPN server through which all the information you're sending and receiving from the Internet passes. Once at the VPN server, the information then goes on to the actual websites or services online that you are using. Much like in the highway example above, someone attempting to view your online activity would only be able to glean that you are using the Internet, not what information you are sending or receiving.

If you're using social media, go to Settings > Privacy and Security > App Tracking, and disable tracking requests.

Change all your social media settings so that no one outside your family and friends can even see your profile. This will keep your profile from being scraped by lots of bad actors and spam producers. When you sign up for apps that require a name and an email address, don't use your real name or the email address that you use for your everyday work and life.

There are services like ProtonMail and Tuta out there that offer free email addresses that are heavily encrypted. Pick a fake name, remember the email address, and every time some service that you want requires your information, use this other address. That will dump all of their spam and advertising towards that account, which you never use.

In the last year, Google has been forcing everyone to use its search to see AI-generated results at the top of the page as the search conglomerate tries to shove AI into everything. Sadly, and rather worrisome, you can't actually turn the feature off, but with browser extensions like the one above, you can hide the results.

A great counterpunch to Google overall is the search engine DuckDuckGo, which doesn't track what you do and forgets your searches as you progress. What a novel approach! If you want everything to be private, not just your searches, opt for a browser like Brave, which has a built-in VPN and specialized code to block all tracking bots that try to attach themselves to you as you scour the Internet for whatever you are looking for.

1. **Routinely clear your browsing data**:
   When you dump the cookies, the cache, and the browsing history, you're also shedding any third-

party bots that are following you on your way across the Internet.

2. **Disable cookies:** You can customize both your browser and your search engines to disable third-party cookies, keeping you from being tracked.
3. **Use browser extensions or privacy browsers:** These let you go about your business without getting harassed by third-party ads and trackers.
4. **You don't need an app for that:** Not every single thing in the world should need to be translated into an app on your phone, stuffed full of your information and waiting to be lifted and used for some other purpose. All those stores that have their own app? They also have stores you can walk up to, websites you can visit, and phone numbers you can call. You don't need an app to figure out how much to tip the waiter or to buy movie tickets either. Remember that these things are tools, not necessities.

With all the information above, you should be relatively secure in your own home, but that's a bit of an issue since we aren't recluses who never go outside. Everywhere we go, we use the Internet—getting directions, ordering from stores, waiting on a flight, on business trips or vacations, etc. Saying "Don't use the Internet" when you're not at home isn't realistic, so we have to go for some other techniques in order to stay safe.

But you also can't trust public Wi-Fi to keep you safe, so either use a VPN or don't use the Internet for anything important—emailing financial information, logging into work servers when you're out and about. Even if you use it for simple tasks, be wary that many hackers will try to set up a second Wi-Fi whose name closely resembles the real one in order to try and trick people into getting on the second one. These are usually someone working nearby who can then start going through every single one of your keystrokes and your history and take what they want.

When you do need to send emails or messages, what you are saying has value, and that value is not meant for everyone. The kind of services you want have wall-to-wall encryption, which means that the message you type is encrypted while it travels to its destination, and only decrypted upon arrival at its destination. Signal and SimpleX are both great examples of chat applications that value your privacy way more than snooping on you.

Remember, it's not just about what you're doing, but where you are.

Don't use social media and other services that announce where you are or want you to check in at a location: Where you are is your business, and you should keep it that way, for your online and personal safety. This is harder to avoid with known face-tracking systems. If you can't avoid them, then wear a hat that covers most of your face or sunglasses to throw the cameras and their AI algorithms off your case and off the scent. It's not about having something to hide, it's about the principle of the thing.

Conclusion

I'd like to say that privacy and surveillance are on a slippery slope, but we all know that's not true. In the past quarter of a century, the slope has turned into a mountain, and it's not just slippery, it's a full-on avalanche towards a very painful bottom. A very painful recurring theme in the history of the Internet and digital technology is rushing to get things to market without really understanding what they are, what they are capable of, what safeguards should be in place, and how they could potentially be dangerous. We are more interested in being first and fastest instead of being safe in the long run. With new technology comes the ability to reach a fork in the road where we decide whether to use it for good or to use it for evil. That's not too strong a word, mind you. When we start using people's mental health records to predict their purchases or spying on baby monitors as children sleep, we've long since left the world of mischievous hackers behind. Instead, we've plunged headfirst into a world of reckless destruction—one driven by power, control, and the fear that if we don't do it, someone else will.

As mentioned in the section comparing our blatant disregard for our own privacy to an addiction, our "use-by-default" compliance is a huge eyesore. Google is as popular as it is because it's convenient and fairly reliable. But the likes of Google, Meta, and Microsoft are finally starting to see some of their market share taken away by companies that understand the value of privacy to consumers, who are finally waking up to the dangers out there and realizing that a lot of them come from the companies who make the technology.

With most technology companies only knowing one way forward—as fast as they can, there are only three presentable options here to cease the current breakneck speed we are on and try to revert to a time where care and compassion weren't just words in a book.

The first way is to play it as "Every man for himself or herself" where we just look out for No. 1, taking the necessary precautions to lower our digital footprint and do the best we can to stay away from the trackers and scrapers of the world.

The second way is to get political. Rally causes. Get on message boards. Write letters to your political representation and attend meetings where privacy, surveillance, and digital Big Brother topics are discussed. Realize that your voice is strong, but that if you don't use it, you have no real business complaining about what is happening in the real world.

The third way is to simply STOP. Stop using apps, websites, and search engines that lie about the way they use your data. Stop buying from brands that are after you solely for your data sets. Stop voting for candidates who are in bed with Big Tech, the ones who couldn't care less whether what they're selling is the best thing since sliced bread or the worst nightmare for privacy. Demand more from the people you put in power—make it clear that your vote is for those who prioritize people over profit, integrity over influence, and your rights over their corporate kickbacks.

We live in a capitalist society, and if we stop using products because we don't like the way they sell our data and spy on us, we can give life to products and services that value privacy by default and engage us with integrity. It's not too late to make this vision into a new reality. The tech in place is not the end-all, be-all unless our lack of caring makes it so. We should desire to give our hard-earned money to corporations with the ethos of caring about its users and data, not turning as big of a profit and selling our data to every bidder out there.

Don't tolerate the way the world is moving and be brave enough to stand fast and not keep being culled along like the rest of the cattle. Speak up, use your voice, and find the words to make others see that right now, everything we do online, in person, on social media, and so on is being done for the benefit of others, not our own. It's time to stop the problem cold in its tracks before every year after 2025 starts to look more and more like 1984.

Remember, there are positive forces out there combatting what the big tech companies are trying to control. Positive forces that don't just want to stop the current path we're on, but reverse it and give people back their anonymity and privacy online. The Googles and Facebooks of the world might be worth billions, but without consumers like us, their power fades quickly—just ask the likes of Yahoo and Myspace. We can work together to forge a way forward to coexist and let everyone feel safe and secure as we head into the future.