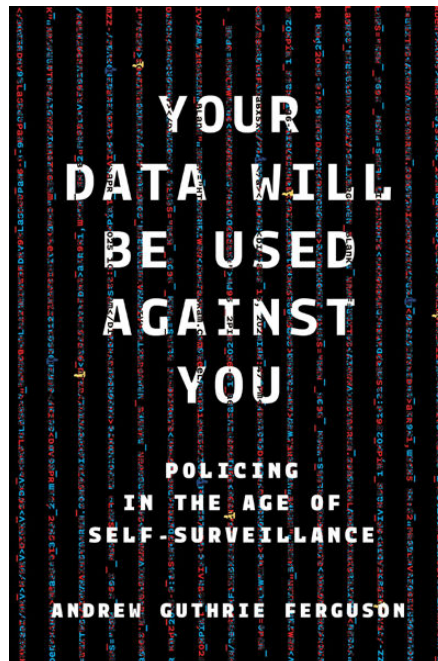


Incriminating Ourselves

J. B. BRANCH

If you've ever felt a creeping unease—*Could I get in trouble for this?*—after asking Alexa a question, texting a friend something deeply personal, walking past a Ring camera, or searching a sensitive question online, Andrew Guthrie Ferguson's *Your Data Will Be Used Against You* is the book for you. More accurately, it is the book that may finally explain why your unease is justified and why our world increasingly feels like an episode of *Black Mirror*.

Modern life puts most of us in the middle of a strange contradiction. Americans recognize that they are being tracked constantly—by corporations, advertisers, platforms, apps, smart devices, cameras, vehicles, and often one another—yet most people still do not fully understand how that data ecosystem functions, who can access it, or how easily it can be weaponized. Surveillance used to be associated with the work of trench-coated government agents conducting wiretaps from vans. It now hides inside sleek packaging,



Your Data Will Be Used Against You: Policing in the Age of Self-Surveillance

by Andrew Guthrie Ferguson. New York, NY: NYU Press, 2026, 320 pp.

personalized recommendations, and the jargon-laden user agreements people are essentially compelled to sign before using software or devices.

Ferguson, a law professor at George Washington University Law School and one of the country's foremost scholars on policing and surveillance technologies, understands that modern surveillance is built through convenience. In his book, Ferguson explores how smart devices, social media monitoring, biometric systems, AI-assisted policing tools, and the endless stream of data people generate about themselves have quietly transformed daily life into a perpetual evidentiary trail that can, in fact, be used against you in a court of law.

What makes the book particularly effective is that it avoids the lazy good-bad binaries that often plague discussions about technology and privacy. Ferguson does not merely rail against the surveillance machine, although he certainly cautions about it, nor does he argue against the

encroachment of innovation and technology into our personal lives. Instead, he acknowledges that many of these technologies can help solve crimes, locate missing persons, identify dangerous actors, and improve public safety. Ring cameras have exposed porch pirates. DNA databases have solved cold cases. Location data have exonerated suspects while simultaneously identifying perpetrators.

But Ferguson's central warning is that the same systems capable of producing safety and convenience also produce unprecedented vulnerability. Smart devices innocently sitting on kitchen counters regularly collect sensitive conversations and noises. Fitness trackers can create a prosecutorial timeline. A car's internal telemetry reconstructs movement patterns. Alarmingly, Ferguson gives real-world examples of pacemakers, search histories, or geolocation data all being used as evidence in court. Readers will become aware of how the world in which we live is surveilled—at times voluntarily, almost always continuously, and often unknowingly.

What distinguishes this book from many others is Ferguson's remarkable ability to synthesize multiple topics well within one text. Too often, books on surveillance narrowly focus on one dimension of the problem, such as consumer privacy or predictive policing. But Ferguson weaves these threads together into a coherent and readable narrative that is accessible without becoming intellectually watered down.

This is a difficult balance to strike. As someone who has spent more than a decade working in legal policy advocacy around criminal justice reform, AI governance, and consumer privacy, I have seen countless experts struggle to communicate these issues beyond academic or technical circles. Ferguson succeeds precisely because he understands that people rarely remember sprawling legal analyses or abstract policy frameworks. They remember stories, examples, hypotheticals, and the

moments that force them to suddenly recognize themselves inside the surveillance machinery being described. *Your Data Will Be Used Against You* is overflowing with such moments.

Nearly every chapter contains memorable hypotheticals and real-world cases that illuminate both the promise and peril of modern surveillance technologies. Some are darkly humorous, exposing the sheer absurdity of criminal behavior. Ferguson recounts, for example, the case of Melvin Thomas, who allegedly brought his cell phone along while stealing valuable construction equipment, searched online for the equipment's value, and later took photographs of himself posing with stacks of cash after selling the stolen goods. Other examples are far less amusing, documenting prosecutorial overreach, sloppy police work, and wrongful suspicion amplified by technologies often treated as objective or infallible. The most unsettling cases reveal how normalized pervasive surveillance has become in American life. Among them is the wrongful arrest of Nijeer Parks, who was identified by an AI-enabled facial recognition system for a shoplifting offense—despite being approximately 30 miles away when it occurred—and jailed for ten days.

The cumulative effect is deeply unsettling. I suspect even readers already immersed in technology policy debates will encounter examples they have never heard before. Ferguson has a talent for stacking revelation upon revelation until the reader begins to recognize that the issue is not isolated to a single technology, rogue company, or police department. Instead, he makes the case that society has created systems capable of documenting nearly every aspect of human behavior while relying on legal frameworks that were never designed for such exposure.

Given Ferguson's expertise as a criminal justice and constitutional scholar, the book is especially strong when unpacking the collision between surveillance technologies and

constitutional doctrine. In assessments that are sophisticated without becoming inaccessible, he demonstrates how analog-era legal assumptions are increasingly strained under the weight of modern technologies. For example, Ferguson illustrates why the third-party doctrine, which allows evidence to be seized if shared with a third-party, is inapplicable when cell phones regularly share personal information with third-party app providers. He achieves this without losing the narrative momentum that makes the book compelling to nonlawyers.

No book can comprehensively solve every challenge it identifies, especially one operating at the intersection of privacy, constitutional law, policing, and rapidly evolving technology. The critiques that follow are therefore less indictments of Ferguson's analysis than reflections on the difficulty of constructing durable safeguards in a surveillance ecosystem that changes faster than law, policy, or book writing can adapt.

For example, Ferguson appropriately emphasizes concepts such as reasonableness, judicial oversight, warrants, and evolving Fourth Amendment doctrine as critical guardrails against abuse. Yet the effectiveness of those safeguards ultimately depends on the attorneys, judges, and courts applying them. American legal history offers numerous examples in which courts have differed dramatically in their interpretation of privacy rights and the power of law enforcement. Given the book's careful attention to technological systems, its recommendations would have been strengthened by a deeper discussion of how judges themselves understand—or misunderstand—emerging technologies and how judicial training might better prepare courts for increasingly data-driven investigations. Ensuring judges possess the technical literacy necessary to evaluate emerging technologies is just as important as crafting new legal standards.

But the book's most notable missed opportunity is its limited discussion of practical steps ordinary readers can take to reduce their own digital exposure. Ferguson excels at helping readers understand how data are collected, aggregated, and ultimately transformed into evidence. He also highlights organizations, advocates, and policy reformers working to address these concerns. Yet many readers will likely finish the book asking, "What can I do to protect myself *now*?"

Step-by-step strategies for reducing one's digital footprint—whether through privacy settings, data broker opt-outs, location controls, account management practices, or other accessible tools—would have provided a better connection between awareness and action. The omission is particularly noticeable because the rest of the book is so successful at translating complex ideas into practical, understandable terms. Readers will be exceptionally well educated about the problem, and many may wish for a similarly comprehensive road map for navigating it. This is not difficult to do: *Wired*, for example, published a frequently cited article that shows readers how to decrease their digital footprints. Ferguson could have offered something similar.

Nevertheless, the strength of *Your Data Will Be Used Against You* comes from its ability to force readers to confront the uncomfortable reality that we live under constant surveillance. It's distributed across platforms, algorithms, data brokers, and consumer devices that millions of people voluntarily invite into their homes every day. Ferguson's central question is whether democratic societies are willing to establish meaningful rules, safeguards, and limits on this surveillance before convenience fully eclipses civil liberties.

That question lingers long after the final page.

J. B. Branch is the Big Tech accountability advocate for Public Citizen's Congress Watch division.