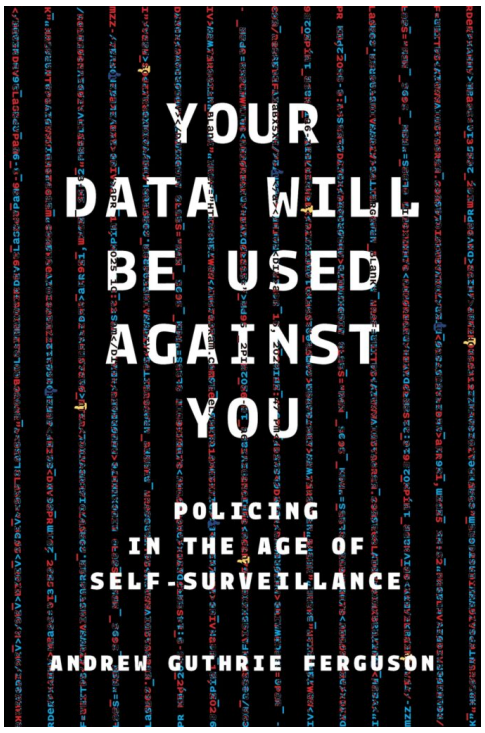
JUST TECH

You Are a Warrant Away from Incrimination

By: Andrew Guthrie Ferguson

SURVEILLANCE TECHNOLOGY



While smart devices—such as smart cars, smartphones, smart watches, and smart medical devices—can assist with and simplify everyday tasks and provide personal insights, the same data this technology uses to help you can be accessed by police and prosecutors looking to find incriminating clues. We are now in a world of self-surveillance with few legal protections.

In his upcoming book, Your Data Will Be Used Against You*, Andrew Guthrie Ferguson explains how the rise of sensor-driven technology, social media monitoring, and artificial intelligence can be weaponized against democratic values and personal freedoms. At the same time, that data will solve crimes, radically transforming how criminal cases are prosecuted. In his introduction, reproduced here, Ferguson lays out examples of potential government exploitation of self-surveillance data to use in prosecution and explains*

how much the law trails technological advances.

The following is excerpted from Your Data Will Be Used Against You: Policing in the Age of Self-Surveillance *by Andrew Guthrie Ferguson (NYU Press). Reproduced with permission.*

I start the class with a question:

"How many of you have used a physical, paper map to travel anywhere in the past year?"

In this group of bright, young law students, no one raises their hand.

"How many of you have printed or written down directions from the internet?"

No hands.

"How many of you have asked a fellow human being for directions in the past year?"

Still no hands.

"How many of you use your phones, or the digital maps in your car, for directions?"

This time, everyone raises their hand.

"How many of you know that the same mapping technologies built into your smartphones and cars are available to police and can be used against you in a criminal case?"

A sheepish hand or two.

"How many of you know that a record of every place you have traveled with that phone is available to police with a warrant?"

Sad looks all around.

"Are any of you going to give up Google or Apple Maps? Or the navigation system in your car?"

Heads shake no. Hands stay down.

So begins a class I teach in law school. The students, like all of us, are trapped by surveillance technology of our own making. We have given data companies—and thus the government—access to our inner lives, and we don't know what to do about it.

This book is about power. It is about how the digital trails we leave behind undermine our privacy and freedom, leaving our most personal information open to police discovery. This book is also about people—because it's the choices we've made to embrace digital convenience and personal security that have created this web of self-surveillance. Every time we step outside our home with a smartphone or ask a smart speaker to play us a song, or Google anything, we create data, and that data reveals who we are.

In a world where everything is data, everything is evidence.

This book is a warning about how the rise of sensor-driven digital technology can be weaponized against democratic values and personal freedoms. This book is not an antitechnology screed. The innovative wonders that put a computer in your pocket or a digital pacemaker in your heart are deserving of respect and consumer attention. But the costs of that innovation are real. We are transforming our physical world and our personal lifestyles with "smart" devices that provide useful data to improve our lives but also reveal them completely. The question is when, if ever, should that smart digital pacemaker in your heart be used as evidence against you in a criminal case. And, it has been.[1]

The simple truth is that digital innovation comes at the cost of digital surveillance. The sensor on your wrist provides personal insights by monitoring you, and that data can be accessed by police and prosecutors looking to find incriminating information.[2] Americans have also bought into the belief that surveillance makes us safer. So, cities invest in networks of cameras instead of community-centered after-school programs.[3] This too is self-surveillance, just mediated by a democratically elected government.

This book explains how you are—at best—a warrant away from having your most intimate personal details revealed to a government agent looking to incarcerate, embarrass, or intimidate you. When your data can be used against you, the government gains power over you and your family in ways that are deeply uncomfortable. All the police need is a judge's signature and everything—from your smart bed to your most embarrassing Google search—becomes evidence.[4] And, even if the government does not make the request, the threat of exposing that data remains ever present.

Two transformations of modern society are just starting to generate the necessary attention and concern. First, this book catalogs the transformation of the built environment—homes, cars, things, and people—into digital tracking devices. The shift is part of an attempt to sell "surveillance as a service" to consumers whereby insights, efficiencies, and patterns become quantified and commodified.[5] Second, this book explores the rise of policing technologies that democratically elected governments are building into cities as affirmative methods of surveillance. The rise of what I have called "big data policing" combines new sensor technologies and old pathologies of surveillance into a new form of social control.[6] This book explores how police and prosecutors are starting to use these two types of information in criminal cases. The intersections are accelerating and will only increase as the digital webs of patterns and habits reveal more of our lives and activities.

This book is grounded in constitutional law and aims to highlight the gaps in legal rules that govern access to the personal data collected by smart devices and public surveillance systems. But in writing it, I also have a higher ambition: to convince you that a world in which you are a warrant away from total digital exposure is not a world you want to live in. No matter how law-abiding or upstanding you consider yourself, the safeguards built into our legal system—search warrants, judicial oversight, concepts like probable cause—are too weak to protect us from the self-surveillance systems we are building. Worse, the commodification of "surveillance as a service"—a billion-dollar industry—provides us a false sense of security, when in fact, it opens our lives to greater intrusion. After all, that digital camera on your door keeping the bad guys away, is also watching you.

Let me begin by telling a story—a modern-day Romeo and Juliet— where two star-crossed lovers find themselves pregnant and living in a state that has criminalized abortion.[7] The couple—privileged, educated, students at a major university—decide to obtain an abortion in a world of digital tracking and sensor surveillance. The tale begins with a Google search outside a sorority house: "Abortion services?" It next involves the car's computer navigation system tracking them travelling from one state to another. (Like my students, using a paper map is not even contemplated.) In addition, the couple's smartphones, and dozens of location-tracking apps all follow the car from the sorority house to a medical facility in a nearby state. Cell site location data reveals precisely how long the couple stayed at the facility. Multiple surveillance cameras, license plate readers, toll records, and a host of other sensors memorialize the trip as well. One need not even add the young woman's smartwatch that is monitoring her vital signs, her Amazon Echo, her period-tracking app, or the texts she sent her worried mother, or even any of her mobile purchases at the drugstore to realize that the web of digital clues about her actions are available to uncover.

If prosecutors discover the couple's intent, investigators can easily scoop up the digital clues. They are investigating a "crime." Many of those pieces of incriminating data do not even require a warrant, but even those that might—a Google search, geolocation data—is just a piece of paper away from being obtained.[8] The couple will be convicted based on the almost inescapable digital clues of their lives. Everyone she communicated with or assisted her is now an accomplice and the subject of criminal investigation with their own digital trails exposed. And, while we might realize in the abstract that digital conveniences come at the cost of digital tracking, we might not realize how easy it is for police to obtain the information once that young couple becomes the target of a criminal investigation.

Photo source: Jeff Trexler/Flickr.

The story is happening somewhere in the United States today. And, if it is not making headlines, that is only because of the relative affluence and privilege of the parties which affords them protection from prosecution. Not everyone will be so lucky. The law is not on their side, and the ease of searching digitally available evidence is rapidly shifting the balance of power toward the government. That same pregnancy story, of course, has happened many times before.[9] In the era before *Roe v. Wade*, illegal abortions were common. Information about practitioners was shared via word of mouth, which meant that marginalized people often had a more difficult time accessing safe, competent care. But it also meant that most people could, and did, end their pregnancies quietly, without leaving a record. There would be no search history, no digital map for looking up directions to a clandestine provider, no geolocation to pinpoint the precise time of the procedure, no texts to a worried mother, no vital signs recorded on a smartwatch. Sure, a police officer could have followed the pregnant person in a car or on foot, but that would require time, effort, and information (knowing the time and date of the procedure, for example), which would have limited the utility of this method of investigation.

What has changed is not just the ease of accessing digital evidence, but also the scale, scope, and ubiquity of existing digital trails.[10] Prosecutors can now search for anyone who has queried a search engine about abortion services and begin an investigation. Police can now geolocate any building that they believe correlates with people seeking abortion services.[11] The existence of digital clues and the

growth of surveillance capabilities cast a wider net on who becomes a target.

The lessons from this story extend to other circumstances in which people might find themselves on the wrong side of those in power: a journalist uncovering political corruption, an employee blowing the whistle on corporate malfeasance, a gun owner buying a new weapon, an undocumented worker, a citizen protesting police brutality, or anyone criticizing the government itself. Digital policing is a godsend for authoritarianism, and in an era where federal and local policing has been weaponized for partisan purposes, the threat of targeted surveillance is all too real. Every perceived political enemy is vulnerable to digital exposure.

Of course, as has long been the reality in the United States, the primary focus of policing will be on the poor and those who commit crimes driven by poverty, addiction, trauma, mental illness, structural inequality, or those lacking education and opportunities to pursue a dif¬ferent path.[12] While crime occurs across socioeconomic strata, and many violent acts cannot be excused by poverty, vast parts of the criminal legal system are focused on policing poverty and ensuring a form of social control over those with lesser economic means. Such has been the history of policing in the United States—with a good bit of overt, implicit, and structural racism thrown in—and such is the future of technology-enhanced, sensor-driven policing.[13] My aim here is not to debate policing. There are many excellent critiques of policing already written.[14] The point is to show how the web of surveillance exploited by the police changes the balance of power between the government and the people—including you.

In the face of this growing digital web, "the law"—the subject I study and teach—has remained decidedly analog. My goal with this book is to alert readers to the danger of that legal stagnation. The lack of legal responses to growing digital privacy threats is a failure of imagination, but also a reflection of other structural inequities in the legal process. Probable cause warrants—the constitutional protection that the Supreme Court has spent countless pages writing about—are weak protections of personal data.[15] Judges are not technologists. Some magistrate judges (who sign probable cause warrants) are not even lawyers.[16] Probable cause is a low standard of proof.[17] And, police control all the information in the warrant, making the judge's role even more limited. It's not that warrants are not important, but they are better thought of as keys to access information, rather than barriers to prevent access.

Second, the book catches us up to the present reality where a world of big data policing filled with predictive analytics, facial recognition, and citywide camera systems create a new surveillance trap.[18] Sensors are not just inside our homes, but also built into our streetlights, listening for gunshots, or automatically reporting on suspicious behaviors.[19] Big cities are erecting AI-assisted surveillance systems capable of long-term, aggregated, pervasive tracking capabilities.[20] Smaller jurisdictions are investing in centralized command centers that seamlessly link license plate readers, video analytics, and suspect lists together.[21] Police body cameras, 911 calls, and private neighborhood social media accounts are used to identify and prosecute individuals.[22] As I will discuss, there are few laws and little regulation around this architecture of structural surveillance.

Combined, the prevalence of private self-surveillance tools and the expansion of public surveillance systems create a world where targeted individuals can find little place to escape. If you cannot claim privacy inside your home or outside of it, you—we—have created a world of enhanced and largely discretionary police power. And, as I will discuss, this power remains unchecked by legal protections and undermined by consumer habits. We live in precarious times when all that stands in the way of digital exposure is a magistrate judge's signature on a piece of paper.

Third, the book examines the costs of digital self-surveillance. The costs include shifts in power, privacy, and privatization, as well as practical problems. When everything is evidence, the government gains power to prosecute, and people also lose a measure of security, autonomy, and community. A federal government with access to unlimited personal data is a recipe for authoritarian abuse. In addition, this surveillance growth strengthens corporate power—vis á vis police—as private platforms distort public safety priorities and community engagement. "Policing as a platform" is not only a marketing pitch, but also a threat to democratic governance. The result is a half-step away from a form of tyranny where those who possess the data can control the citizenry. "Tyranny" is a rhetorically loaded word, but the reality of an all-controlling, ever-observing digital power is not too far a stretch in an era of politized prosecution.[23] Finally, self-surveillance comes with a host of practical problems including how data is used, misused, and just gets things wrong. For every program that seeks to turn data into usable intelligence, there are a dozen scandals about how the data is wrong, conflates causation and correlation, or is racially biased against certain communities.[24]

Lastly, the book offers solutions to a world where everything is evidence that will be used against you. Perhaps not surprisingly, the response also takes everything into account. Constitutional limitations require a judicial response that expands Fourth Amendment understandings to suit the digital age. Legal limitations require federal, state, and local legislative responses to fill the gaps around consumer data

and police use of new surveillance technologies. Impacted communities must be given a voice through the creation of local mechanisms of community control. We must heed abolitionist warnings about the foreseeable abuses from technologies of social control. And, finally, individuals must be empowered to reshape consumer demand for self-surveillance technologies that put data controls and destruction in the hands of the users and not with the companies. There is no reason why sensor surveillance data must be retained, or accessible by anyone but the user. Technology must pass what I call "the tyrant test," and if it fails, it should not be sold or used.[25]

Today, criminal prosecutions look pretty similar to the court practice of the past century. Prosecutors rely on human witnesses and physical evidence. Cell phones and social media posts make an appearance. Forensic evidence—most obviously DNA—has become a routine part of many serious cases.[26] But digital forensics—proving a case with the digital clues of life—is only just becoming common enough to generate concern. In the near future, this will change, and criminal courtrooms will be filled with digital evidence generated by our smart things and the surveillance world around us. This book explores how we should understand that change and adapt to it. It also seeks to warn about what might happen if we ignore the growing surveillance systems increasingly integrating into our lives.

The overarching goal of this book is to contribute to the national conversation around surveillance, privacy, power, and law. But I also hope you'll find it relevant to you personally. If you think about all the data you put out into the world—data that reveals your interests, desires, habits, and connections in intimate detail—you will see that these issues directly affect your life and the lives of your loved ones. While this book is filled with stories about criminal wrongdoers getting caught because of their digital trails, the surveillance net captures everyone. Who is deemed "criminal" is a contested and changeable reality.[27] Politicians can easily demonize individuals and groups, turning surveillance against citizens. Technologies developed to thwart violent crime can be repurposed for political repression. American history—from revolutionaries, to abolitionists, to draft avoiders, to dissenting religious, cultural, and political voices—is filled with stories about people who were convicted based on hatred, ignorance, or prejudice.[28] And to put a finer point on it—all of those people would have been far easier to prosecute with the digital evidence now available.

All that said, police are using our data to catch people who have done truly awful things. Depending on how you view police power, you may read this book's various vignettes of dumb criminals and smart data as evidence that these technologies are a great gift to criminal justice. Murderers are caught. Innocent people are exonerated. Data proves the truth, or at least eventually gets to the right result.

The uncomfortable reality is that the national conversation is not one-sided. Both the promise of new technologies and their dangers are very real. Part I offers a window into how criminal prosecution is changing in response to digital technologies of self-surveillance. Part II examines the real risks of this shift, focusing on changes in power, privacy, and criminal justice practice. Part III offers solutions to the problems raised in the book, with a focus on what judges, legislatures, and individuals can do to respond to the risks.

Despite its complexity, the debate over new policing technologies is an urgent conversation to begin. We all need to engage in the debate so that we can get the rules right when it comes to surveillance power. Especially now, as federal power expands and politicized prosecutions grow more common, the danger of doing nothing becomes intolerable. The laws governing digital evidence are still unwritten. And for every minute we spend waiting, the net of self-surveillance we've trapped ourselves in grows tighter. How or whether we escape that net will be up to us. I hope this book helps point the way out.

Footnotes

1 Cleve R. Wootson Jr., "A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story," *Washington Post*, February 8, 2017, https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story/.

2 See, e.g., Scott R. Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent," *Texas Law Review* 93 (2014): 93.

3 See Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press, 2017), 190.

4 *People v. Seymour*, 536 P.3d 1260, 1273 (Colo. 2023).

5 See Alison Griswold, "Amazon Wants to Sell 'Surveillance as a Service'," *Quartz*, June 20, 2019, https://qz.com/1648875/amazon-receives-us-patent-for-surveillance-as-a-service.

6 See Ferguson, *The Rise of Big Data Policing*.

7 See Alejandra Caraballo et al., "Extradition in Post-*Roe* America," *CUNY Law Review* 26, no. 1 (Winter 2023), https://academicworks.cuny.edu/clr/vol26/iss1/3/.

8 See Paul Ohm, "Probably Probable Cause: The Diminishing Importance of Justification Standards," *Minnesota Law Review* 94, no. 5 (2010): 1515, https://scholarship.law.umn.edu/mlr/507/.

9 Cynthia Conti-Cook, "Surveilling the Digital Abortion Diary," *University of Baltimore Law Review* 50, no. 1 (2020), https://scholarworks.law.ubalt.edu/ublr/vol50/iss1/2/.

10 Jennifer Daskal, "Notice and Standing in the Fourth Amendment: Searches of Personal Data," *William & Mary Bill of Rights Journal* 26, no. 2 (2017): 454, https://scholarship.law.wm.edu/wmborj/vol26/iss2/9/.

11 See Aziz Z. Huq and Rebecca Wexler, "Digital Privacy for Reproductive Choice in the Post-*Roe* Era," *NYU Law Review* 98, no. 2 (2023): 574, https://nyulawreview.org/issues/volume-98-number-2/digital-privacy-for-reproductive-choice-in-the-post-roe-era/.

12 Paul Butler, *Chokehold: Policing Black Men* (The New Press, 2017), 59–61.

13 See generally Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Polity, 2019); Alex S. Vitale, *The End of Policing* (Verso, 2017); Angela Davis, ed., *Policing the Black Man: Arrest, Prosecution, and Imprisonment* (Vintage, 2017); Michelle Alexander, *The New Jim Crow: Mass Incarceration in the Age of Colorblindness* (The New Press, 2010).

14 See Benjamin, *Race After Technology*; Vitale, *The End of Policing*; Davis, *Policing the Black Man*; Alexander, *The New Jim Crow*.

15 Barry Friedman, *Unwarranted: Policing Without Permission* (Farrar, Straus and Giroux, 2017), 143–84.

16 Craig S. Lerner, "The Reasonableness of Probable Cause," *Texas Law Review* 81, no. 4 (2003): 981–95.

17 Matt Ford, "When Your Judge Isn't a Lawyer," *The Atlantic*, February 5, 2017, https://www.theatlantic.com/politics/archive/2017/02/when-your-judge-isnt-a-lawyer/515568/.

18 See generally Ferguson, *The Rise of Big Data Policing*, 190; Andrew Guthrie Ferguson, "Facial Recognition and the Fourth Amendment," *Minnesota Law Review* 105, no. 3 (2021): 1115, https://scholarship.law.umn.edu/mlr/3204/.

19 See generally Ferguson, *The Rise of Big Data Policing*, 190; Ferguson, "Facial Recognition," 1115; see also Andrew Guthrie Ferguson, "Structural Sensor Surveillance," *Iowa Law Review* 106, no. 1 (2020): 57, https://ilr.law.uiowa.edu/print/volume-106/structural-sensor-surveillance.

20 Andrew Guthrie Ferguson, "Persistent Surveillance," *Alabama Law Review* 74, no. 1 (2022): 5, https://law.ua.edu/wp-content/uploads/2025/03/1-Ferguson-1.pdf.

21 Zac Larkman, "The Quiet Rise of Real-Time Crime Centers," *Wired*, July 28, 2023, https://www.wired.com/story/real-time-crime-centers-rtcc-us-police/; Jay Stanley, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy* (ACLU, 2019), 17–21, https://www.aclu.org/publications/dawn-robot-surveillance.

22 Brandon Block, "Federal Aid Is Supercharging Local WA Police Surveillance Tech," *CrossCut*, Cascade PBS, July 26, 2023, https://www.cascadepbs.org/investigations/2023/07/federal-aid-supercharging-local-wa-police-surveillance-tech/; Rachel Levinson-Waldman, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media," *Oklahoma Law Review* 71, no. 4 (2019): 998, https://digitalcommons.law.ou.edu/olr/vol71/iss4/2/.

23 Jahd Khalil, "Real Time Crime Centers, Which Started in Bigger Cities, Spread Across the US," NPR, August 16, 2023, https://www.npr.org/2023/08/16/1194115202/real-time-crime-centers-which-started-in-bigger-cities-spread-across-the-u-s; Jim McKay, "Crooks Can't Dodge the Real-Time Crime Center 'Double Click'," *Government Technology*, December 7, 2023, https://www.govtech.com/em/crooks-cant-dodge-the-real-time-crime-center-double-click.

24 Eva Ruth Moravec, "Do Algorithms Have a Place in Policing," *The Atlantic*, September 5, 2019, https://www.theatlantic.com/politics/archive/2019/09/do-algorithms-have-place-policing/596851/; Will D. Heaven, "Predictive Policing Is Still Racist—Whatever Data It Uses," *MIT Technology Review*, February 5, 2021, https://www.technologyreview.com/2021/02/05/1017560/predictive-policing-racist-algorithmic-bias-data-crime-predpol/.

25 Andrew Guthrie Ferguson, "Surveillance and the Tyrant Test," *Georgetown Law Journal* 110, no. 2 (2021): 208, https://www.law.georgetown.edu/georgetown-law-journal/in-print/volume-110/volume-110-issue-2-december-2021/surveillance-and-the-tyrant-test/.

26 Kerry Abrams and Brandon L. Garrett, "DNA and Distrust," *Notre Dame Law Review* 91, no. 2 (2015): 758, https://scholarship.law.nd.edu/ndlr/vol91/iss2/6; Erin Murphy, "License, Registration, Cheek Swab: DNA Testing and the Divided Court," *Harvard Law Review* 127, no. 1 (2013): 180, https://harvardlawreview.org/print/vol-127/license-registration-cheek-swab-dna-testing-and-the-divided-court/; Erin Murphy, "Relative Doubt: Familial Searches of DNA Databases," *Michigan Law Review* 109, no. 3 (2010): 294, https://repository.law.umich.edu/mlr/vol109/iss3/1/.

27 Alec Karakatsanis, "Why "Crime" Isn't the Question and Police Aren't the Answer," *Current Affairs*, August 10, 2020, https://www.currentaffairs.org/news/2020/08/why-crime-isnt-the-question-and-police-arent-the-answer.

28 After all, even the Founding generation was involved in criminal activities like smuggling and tax evasion. Kiel Brennan-Marquez and Stephen E. Henderson, "Search and Seizure Budgets," *UC Irvine Law Review* 13, no. 2 (2023): 404, https://escholarship.org/uc/item/61v348ww.