THE INFORMATION TRADE

THE INFORMATION TRADE

How Big Tech Conquers Countries, Challenges Our Rights, and Transforms Our World

ALEXIS WICHOWSKI

HarperOne
An Imprint of HarperCollins*Publishers*

FIRST EDITION

Designed by Joy O'Meara and Lucy Albanese

Library of Congress Cataloging-in-Publication Data has been applied for.
ISBN 978-0-06-288898-3

20 21 22 23 24 LSC 10 9 8 7 6 5 4 3 2 1

To Jonathan, for being mine.
To Gerome, Novi, & Leo, for being all your own.

Where, after all, do universal human rights begin?
In small places, close to home—so close and so small
that they cannot be seen on any maps of the world . . .
Unless these rights have meaning there,
they have little meaning anywhere.
Without concerned citizen action to uphold them close to home,
we shall look in vain for progress in the larger world.

—ELEANOR ROOSEVELT,
former first lady of the United States

We don't completely blame Facebook.
The germs are ours, but Facebook is the wind,
you know?

—HARINDRA DISSANAYAKE,
Sri Lankan presidential adviser

CONTENTS

INTRODUCTION

On January 9, 2007, 45,000 software developers, computer engineers, and everyday tech enthusiasts gathered in Silicon Valley's go-to conference spot, San Francisco's Moscone Center, a three-story, glass-enclosed conference space that shared a block with the Yerba Buena Ice Skating and Bowling Center and the Dosa Brothers Indian restaurant. The occasion: the 22nd annual Macworld Expo. The highlight: bearing witness to their patron saint, Apple visionary Steve Jobs.[1]

Wearing his signature uniform—black turtleneck, wire-frame glasses, white sneakers, and blue jeans—Jobs took to the stage. A giant backlit Apple logo loomed on a wall-size screen behind him.

Twenty-two minutes into a speech sprinkled with updates about various Apple products, Jobs stopped. A moment of silence passed. "This is a day I've been looking forward to for the past two and a half years," he announced.[2] Scattered applause peppered the room, but Jobs waved it away.

With something like defiance, he declared, "The most advanced phones are called 'smartphones,' so they say." The audience burst into laughter. In 2007, when most people still carried flip phones and PDAs,

the very notion of such a thing seemed absurd. Jobs went on to blast then-current "smartphones"—BlackBerries and Nokias, namely—as being difficult to navigate, even for basic functions. "What we want to do is make a product that's way smarter than any cell phone *and* that's easy to use. This is what iPhone is."

The iPhone launch is worth cherishing. It may very well have been our last mass-magical tech moment, a time when the entire world got truly excited over a technological breakthrough.

This was a time before tech got scary.

It was almost four years before WikiLeaks released 251,287 diplomatic cables to the press, which contributed to the bloody and largely unsuccessful Arab Spring and drove home the terrible power and scale of leaks now possible in the digital age.[3]

It was six years before Edward Snowden's revelations shattered public trust in the US government by unveiling the National Security Agency (NSA) mass covert data collection program that sought info on American citizens.

It was almost a decade before the Russian military's Information Research Agency infiltrated the 2016 US presidential election through misinformation warfare, peeling away the belief that our social networks consisted of our friends, or at the very least, our compatriots.

And it was eleven years before Facebook was outed for giving political consulting firm Cambridge Analytica access to 87 million users' data, finally tipping the world's wide-scale disillusionment with the tech industry into outright anger.[4]

In 2007, we still loved our tech and its keepers. The proof is in the purchases. Half a million people bought iPhones the first weekend they were available.[5] Buyers lined up around the US—for days, in some places.

"I feel wonderful. It's exhilarating," reported 51-year-old engineer David Jackson as he finally held an iPhone in his hands, having waited in line more than 24 hours for the moment. "Man, that was cool. I was shaking at the counter. I couldn't even sign my name."[6]

With the iPhone, Apple gave us what seemed like one of the greatest

godsends of the digital era: a keyboardless, full-color, internet-enabled, do-everything device—one that was pretty and sleek and fit in your pocket, to boot.

We may not have recognized it at the time, but Apple did more with the iPhone than create a next-generation personal computer. They created the first *wearable* computer: a device that you could keep on your body, in your pocket, at all times. In 2019, this was a reality for roughly 2 billion smartphone users, whether they carried an iPhone or its chief competitor, an Android (Google) phone.[7] The smartphone didn't just make life easier; it didn't just make us, as Apple's '90s-era slogan urged, "think different." It made *life* different.

ALMOST EXACTLY 10 YEARS AFTER JOBS INTRODUCED THE IPHONE TO the world, another tech luminary addressed a similarly massive audience at the Moscone Center—for quite different reasons.

On Valentine's Day 2017, Brad Smith—the affable, sandy-haired president of Microsoft—took the stage at the annual RSA Conference, the tech industry's premier security conference. "Cyberspace," he declared, "is the new battlefield."[8]

"The world of potential war," he warned, "has migrated from land to sea to air and now cyberspace. As a global technology sector, we need to pledge that we will protect customers." He paused. "We will focus on defense."

Let's take a moment to digest this. The president of Microsoft—*Microsoft*, the company whose products are virtually synonymous with corporate cubicle culture—announced to 40,000 of the tech industry's frontline programmers that they were, for all intents and purposes, at war.

"Because when it comes to attacks in cyberspace, we not only are the plane of battle, we are the world's first responders." He continued, "Instead of nation-state attacks being met by responses from other nation-states, they are being met by us."

Let's see that again: "They are being met by *us*."

Who is "us"?

Smith was talking about something new—some higher-order embodiment of digital power. These new entities are tech companies' next stage of evolution, a giant technological leap from Jobs's iPhone.

These tech entities are no longer simply making spreadsheet software and calendar apps and gadgets. They are battlefields. They are weapons. And, most important, in this speech Smith declared that these new entities should be—must be—a force for good.

The problem here is that no one knows what to call these new things. As I first introduced in a 2017 *WIRED* article, I propose that we call them "net states."[9]

Why not just keep calling them "the tech industry"? The short answer is that the tech industry is no monolith, with all its companies pursuing the same goals with the same business practices.

As hard as it may be to think of the world's newest industry as traditional in any way, a handful of "traditional" companies have undergone a metamorphosis. And, in the same way we don't keep calling butterflies "caterpillars" once they've transformed, these particular companies—Amazon, Apple, Facebook, Google, Microsoft, and Tesla, specifically—have morphed into something altogether different from "the tech industry."

They no longer only make products and offer services. They're reaching beyond their core technologies to assert themselves in our physical world. They're inserting digital services into our lived environments in ways both unseen and, at times, unknown to us. And, most important, they're exerting formidable influence over the way our world works on individual, societal, and geopolitical levels. *These* tech companies are unlike anything we've encountered before.

Net states vary in size and structure but generally exhibit four key qualities: They enjoy an international reach. Their core work is based in technology. Their pursuits are influenced, to a meaningful degree, by beliefs, not just a bottom line. And, perhaps most significant, they're

actively working to expand into areas formerly the domain of governments, areas that fall outside their primary products and services—areas they pursue at times separate from and even above the law.

Simply put, net states are not just out to make widgets or get people hooked on a single product. (This is why Tesla and its world-building businesses are included in the book and Twitter, with its single, standalone platform, is not.) Net states are out to change the world—not just in theory, but in defense, diplomacy, public infrastructure, and citizen services.

Net states are tech entities that act like countries. By acting like countries, net states alter our experiences as citizens. And they alter countries' experiences as geopolitical powers.

Two examples—Silk Road and Project Maven—show this in action.

"IT IS WITH A HEAVY HEART THAT I COME BEFORE YOU TODAY," WROTE a user, code-named Libertas, in his farewell letter.[10] "A heart filled with sadness for the infringements of our freedoms by government oppressors." He wrote, "Silk Road has fallen."

Libertas was the Roman embodiment of freedom; the inspiration for the Statue of Liberty. It was also the pseudonym Gary Davis used on Silk Road—not the historic trading route in Central Asia; the illegal marketplace on the dark web that freely sold everything from drugs to hacking-for-hire services to humans from its launch in January 2011 to October 2013, when the FBI shut it down.[11]

Davis worked as a low-level site administrator for Silk Road—the Mafia equivalent of a bookie. Admin though he was, Davis hardly looked like a stereotypical hacker, showing up at his trial sporting a trim suit, well-groomed chinstrap beard, and seemingly well-rehearsed thousand-yard stare.[12] While Davis was a minor figure in the Silk Road case, Silk Road itself was a major problem that had dogged the FBI for years. It thrived, selling illegal wares in plain view of the authorities to its consumers, who spent more than $1.2 billion in its two-plus years

of operation.[13] Yet with all transactions encrypted via Bitcoin, the authorities couldn't figure out who was running it. When the FBI finally cracked the case, they scooped up everyone they could find associated with the site, including lowly admins like Davis.

On December 19, 2013, at 8 p.m., at the behest of the FBI, Irish authorities swooped into Davis's hometown of Wicklow, a sleepy seaside town about an hour southwest of Dublin.[14] Finally, after two long years of failed attempts to shut down the site, it looked as if the Silk Road case was under control: the FBI had found their suspects, and it was only a matter of time before they gathered the material evidence needed to put them away.

Then the investigation hit a brick wall. While Davis used an encrypted browser called TOR for his Silk Road–related work, he preferred Microsoft for his personal emails, which meant that Microsoft, whether they were aware of it or not, had been safeguarding content for an international drug trafficker.

As a matter of routine, the FBI got its subpoena for the emails and handed it over to Microsoft. But then, something unusual happened: Microsoft stalled. Because while Microsoft now knew they harbored content belonging to a probable felon, technically they were *allowed* to: since Congress had passed the Communications Decency Act in 1996, tech companies couldn't be held legally responsible for the content on their platforms.[15]

The issue for Microsoft wasn't the particular user the FBI was after, or even the potentially incriminating content of his emails. The problem was that the emails weren't stored in United States territory. They were on a server in Dublin, Ireland. And whether an American subpoena had jurisdiction over data physically housed on machines in another country simply wasn't clear.

So while Microsoft handed over the Davis emails physically stored in the United States, they declined to turn over the ones housed in Ireland.

In sum, Microsoft, an American-based tech firm owned and operated by American citizens, refused to comply with the American

government's subpoena. And amazingly enough, they weren't breaking any laws, because none existed at the time that made clear what the appropriate course of action should be.

In 2013, the US Department of Justice sued Microsoft to retrieve the Dublin-stashed emails.[16] That case turned into a fiasco. What might have been a simple paper chase became a many-year legal crusade. Because for Microsoft, it was never about Davis, or even the content of his emails. This was the case that would set precedent for the US government's jurisdiction over global digital communications for years to come. As of this writing in 2019, the case is still making its way through appeals courts.

On one level, the Silk Road story is about citizens' rights online: who gets to decide what happens to digital information, the tech companies who manage user data or the countries in which the users reside. But on another, it's about citizens' rights in real life: which entity gets to decide the fate of that user, a fate that might come with stakes as high as physical imprisonment.

Surprisingly, of the three players involved in this fight—two countries (the United States and Ireland) and one tech company (Microsoft)—the tech company, not the countries, took the lead on safeguarding citizens' rights.

To be fair, the American government is legally beholden by the Constitution to "pursue justice" on behalf of *its* citizens. Which they did, attempting to convict perpetrators whose illegal marketplace harmed untold numbers of victims. But on the other hand, the American government is also constitutionally prevented from conducting "unreasonable searches and seizures." Microsoft could conceivably argue that this is what the US government was doing, as the desired objects of the searches were physically outside US territory.

The elephant in the room is, of course, that while this may *technically* be the case, this is not in any way *practically* the case. It's not like Microsoft would have had to send a team of experts across the Atlantic to excavate documents with a trowel. It could have conjured up the

Dublin emails with the mere click of a button, never having to leave its headquarters in Redmond, Washington.

The question is, then, why Microsoft went through the bother. Legal cases are extremely expensive, even for tech empires. And they're time-consuming; this case has dragged on for over six years already. But most important, unlike governments that are constitutionally bound to look after their people, Microsoft—or any other tech company, for that matter—has no obligation to put up any sort of fight for citizens' rights.

Then a rationale begins to emerge: Microsoft's not actually protecting *citizens*; they're protecting *users*. They're not securing citizens' physical belongings from "unreasonable search and seizure." They're protecting their users' data.

In this way, "citizen" and "user" merge in some information-age mashup, becoming something new: the "citizen-user." Because whether Microsoft is really protecting "citizens" and their rights or protecting "users" and their data is almost irrelevant. The end result is the same: the tech company is standing up for the individual. And in this particular case, the United States, the most powerful country on Earth, can't do a thing about it.

This shows how major tech companies can outmaneuver countries—how they operate above the laws of individual countries. This is how tech companies become net states.

OUTMANEUVERING COUNTRIES ISN'T ALWAYS FUELED BY LEGAL MURKIness or precedent-setting. Sometimes, it's a matter of plain old principle: net states refusing to work with governments because it goes against their beliefs, even when it means losing money.

"It's so exciting that we're close to getting MAVEN!" wrote Google Cloud's chief scientist for artificial intelligence (AI), Fei-Fei Li, in an email obtained by the Gizmodo Media Group.[17] The "MAVEN" Li refers to would be "Project Maven," the plain English moniker for the Department

of Defense's (DOD) exploratory artificial intelligence program.[18] Maven's mandate was essentially to put AI capabilities on drones.

"I think we should do a good PR on the story of DoD collaborating with GCP from a vanilla cloud technology angle (storage, network, security, etc.), but avoid at ALL COSTS any mention or implication of AI," Li's email continued, urging her colleagues to steer clear of what could be a public relations nightmare. She instead pitched Project Maven as a "vanilla"—in other words, harmless—cloud storage partnership. This shows how even in those early planning days, Li was conscious, and nervous, about what would happen if the public thought Google was collaborating with the Department of Defense on anything to do with artificial intelligence. As her email suggested, it wouldn't be difficult for this to quickly spiral into "killer robots" headlines splattered across the news.

Turns out the media wasn't Google's main problem. Rank-and-file Google employees would prove to be the project's undoing.

Before getting to Google employee protests, it's important to dig beyond the perception of Project Maven and look at what Project Maven actually aimed to do. Maven's AI was supposed to aid human operators at DOD sift through massive troves of information, "to help a workforce increasingly overwhelmed by incoming data, including millions of hours of video." And no one within DOD had developed AI to the point where it could be deployed in this way. As Colonel Drew Cukor, chief of the Algorithmic Warfare Cross-Functional Team responsible for Project Maven, announced at the Defense One Tech Summit in 2017, "You don't buy AI like you buy ammunition. This effort is an announcement . . . that we're going to invest for real here. The only way to do that is with commercial partners alongside us."[19]

It started as a tiny project, in Google terms. The $9 million contract, which launched in 2017, involved just 10 employees, a minuscule allocation of resources from Google's 88,000-person workforce.[20] But as word about Project Maven spread throughout the company over the next several months, outrage ensued. About a dozen AI researchers at Google

resigned in protest, the first mass resignation over a matter of principle in Google's history.[21] This was shortly followed by a petition signed by 4,000 staffers demanding that Google cease its AI contract with the military immediately.

"We believe that Google should not be in the business of war," began the one-page letter to Google's CEO, Sundar Pichai.[22] "Building this technology to assist the US Government in military surveillance—and potentially lethal outcomes—is not acceptable."

Most notable, however, was not the fact of the petition or even that it demanded an end to Google's partnership with the Pentagon; it was the workers' rationale for the protest. "We cannot outsource the moral responsibility of our technologies to third parties," the letter stated. "Google's stated values make this clear: *Every one of our users is trusting us. Never jeopardize that. Ever.*"

The resignations and petition worked. Despite the potential financial windfall future military contracts could bring the company, on June 1, 2018, Google announced that it would not be continuing the Project Maven contract once it expired at the end of the year.

WE'RE IN A WORLD STILL DOMINATED BY NATION-STATES, BUT INCREASingly influenced by the actions of net states. Nation-states continue to own the physical territories within their borders, but net states wield significant power both within and across country space, guiding events that affect us both on an individual and on a global level. Therefore, we need to get smart about what net state power really looks like, and quick.

One country that's excelling in its efforts to do so is Denmark. In 2017, it opened a door that has the potential to radically alter our existing geopolitical order: it appointed a new ambassador to capital-T Tech itself. Ambassador Casper Klynge is the world's first-ever tech ambassador. His mandate: to establish diplomatic relations between Copenhagen and Tech. And what exactly *that* looks like is all fresh territory, yet to be discovered. Fittingly, his office operates as a virtual embassy, with

three physical manifestations: one in his home base of Copenhagen and two in the most powerful tech hubs on Earth—Silicon Valley, California, and Beijing, China.

I arranged to interview Ambassador Klynge from his Silicon Valley office in late April 2019. I'd given his communications director my cell number and sat on the sofa in my basement home office in Brooklyn, waiting for the call. The lights were off, the only source of illumination being the gray-white glow from my computer screen. (This was deliberate; frankly, I didn't want to be distracted looking at laundry piles in the corner during the interview.)

Suddenly, my phone rang. But in addition to ringing, the screen lit up, serving up an image of my own face as well.

Oh. We're having a *FaceTime* interview, I realized. I should have expected it—tech ambassador, after all. Because I didn't want to miss the call, I answered before I had time to turn on the light. Two tanned, cheerful people greeted me on what appeared to be a sunny day in a naturally lit office somewhere in Silicon Valley, their friendly faces framed by a whiteboard with vague scrawl in the background.

"Are you . . . um, is this still a good time?" Ambassador Klynge asked encouragingly. I could see in the tiny window FaceTime provides of one's own reflection the eerie computer light cast on my face, giving me a ghostlike appearance. Despite this less than ideal setup, it had taken quite a bit of work to get on the ambassador's calendar, and I didn't want to miss my chance. So, there we were—I in my dark Brooklyn basement and he in his sunny California diplomatic outpost—talking, smiling through our cell phones.

I went straight for my most pressing question first: He's the world's first ambassador to the tech sector—how had that sector received him?

Ambassador Klynge's expression made it seem as if this question brought a story to mind. Having worked with diplomats in my past, I doubted I would hear it in an on-the-record conversation like this, though, and didn't press. After a moment, he said that "some companies" had been "very forward-leaning." He paused. "Then you have the

other side of the spectrum," he said, "where some companies have been enormously difficult to deal with. . . . We deliberately say we want more or less to come in at the top level. That means C-suite level, and they sort of offer the oldest intern. . . ."

The ambassador trailed off for a second. On the screen, I could see Klynge lean slightly forward at his conference room table, pinning his index finger to some invisible spot on it. "I think *reluctant* is a very diplomatic term."

I wanted to ask which companies sent an intern to greet him—an ambassador!—but didn't think he would be at liberty to disclose. I figured I could probably guess for myself anyway: for this book, Microsoft and Google happily accepted my interview requests; Facebook, on the other hand, was a vault.

What about governments? I asked. Were they reluctant as well?

Total opposite, he said without hesitation.

"There has been enormous—I would almost say *unprecedented*—interest from other capitals in basically learning from us, getting our experiences from dealing with the tech industry." He said, "They tell us, 'We would love to do something similar [to your tech embassy], but our bureaucracies are so large and so difficult that we would never be able to do it; . . . the distance from *flash* to *bang* is simply too big.'"

Then Klynge's whole face lit up; he was clearly pleased to reflect on what his country had been able to accomplish. "That's one of the areas where being small is a little bit of an advantage."

This comment revealed a distinct advantage Denmark and the two other countries who've since appointed their own tech ambassadors—Estonia and Australia—have over their larger nation-state counterparts. When it comes to tech, the smaller nations have proven to be like speedboats amidst a sea of ocean liners. Nation-state behemoths may still have more firepower and financial might, but, essentially moored in place by their unwieldy mass and unforgiving bureaucracies, they can't seem to keep up with net states nearly as well as countries like Denmark and Estonia.

I had time for one last question. How should we—governments, societies, people like you and me—be thinking about technology? How do *you*, Mr. Tech Ambassador, see it?

He took just a moment, barely a beat—it could have been a hiccup in our connection, really. But then he said, "The freight train is coming."

Klynge continued, "It might not be everybody who's seeing the massive impact of technology also on international relations, but one of the reasons why we gather . . . countries [is] to try and help shape thinking in capitals all over the world."

Governments need to understand, Klynge explained, that technology is much more than "an add-on." "It's not the IT office that needs to deal with technology; it's mainstream foreign and security policy."

I invited him to explain why he thought so, and this time he responded immediately. "Technology will have a massive impact on international relations. It will have a massive impact on the convening power of the West. It will have a massive impact on the balance of power in the future," he said.

Then he added one last thought. "For *that* lesson, it's high noon for many, many countries all over the world."

Casper Klynge and his fellow tech ambassadors exist because at least three of the world's most forward-leaning countries have come to recognize, in the most formal and official way a country can, that net states occupy a substantial role in our geopolitical, social, and personal worlds. This book describes the various ways in which net states exert influence on those worlds and each of us in them, as well as what we can—and must—do to ensure that they do so responsibly.

This book shows us our tech in a new light: not just as services we access or devices we use but as forces of personal, social, and geopolitical power. From this new vantage point, we gain additional ground for exploration: the capacity to ask questions about tech's impact that we've yet to even consider.

This book is not an exposé of any individual net state, though the major tech companies serve as our main characters. It's the story of what

net states are up to, both as they engage with us—their citizen-users—and as they expand out of the digital and into the physical world.

THIS BOOK STARTED WITH AN ARTICLE I WROTE IN 2015 AND LEFT IN a file for two years. I wrote it to try to make sense of what had happened following the November 2015 terrorist attacks in Paris. The day after those attacks, the hacker collective Anonymous launched a campaign, Operation ISIS, in which they claimed to have taken down upwards of 20,000 ISIS-related social media accounts in a single day.[23] By comparison, the social media companies themselves had taken down only around 800 ISIS accounts over the prior 18 months.[24]

It occurred to me that the social media giants and Anonymous both had a bigger role to play in fighting terrorism than I'd seen discussed. But I ran into a problem: *how* to discuss it. What *was* Facebook? And Google? And Anonymous? And the other major tech companies and movements? They clearly weren't nation-states, like the US and France. But they weren't nonstate actors, like ISIS or al-Qaeda, either. We simply didn't have the language at the time to categorize them. Despite that, it was becoming increasingly evident that these . . . somethings . . . were forces to be reckoned with—not just as commercial entities but as significant players in defense, diplomacy, and other geopolitical arenas.

When I shared the draft article with my most trusted readers, it elicited raised eyebrows—one Anonymous campaign did not seem quite sufficient to support a new theory. So I shelved the piece but kept collecting evidence: examples of incidents in which tech companies had reached beyond their core services and into governmental areas. By 2017, I felt I had gathered enough data to warrant dusting off the article and making the public case for net states. *WIRED* magazine agreed: in November 2017, it published "Net States Rule the World: Ignore Them at Your Peril," introducing the term "net states" to the lexicon.

Since 2017, evidence that tech companies are acting like countries has only continued to amass. In June 2019, Facebook announced the

launch of its own monetary project: a cryptocurrency, Libra. As technologist Micah Sifry observed in his newsletter, *Civicist*, "If you're going to be a country, you might as well have a currency, right?"[25]

The Information Trade is both a near history and a profile of what it means to live a tech-enabled life. It celebrates how technology enables us to share the stuff of life—information, data, stories, knowledge, sorrows, silliness, and ephemera. It informs us about what happens to that data when we do share, both with and without our knowledge. And it cautions us against giving up our ability to influence the balance of power between ourselves, our governments, and our net states.

"NET STATES" IS KIND OF LIKE "SEA CREATURES" OR "THE EUROPEAN Union": it's a label that represents a larger group. Its members share features, but there's a lot of variation among them. In the same way you wouldn't want to read a book about sea creatures without learning about sharks and whales, or a book on the EU without touching on Germany or France, this book is structured around five major net states—Amazon, Apple, Facebook, Google, and Microsoft—as well as the net state activity exhibited by Elon Musk's Tesla and its sister projects, and the political movement represented by independent Pirate Parties in various countries.

Chapter 1 looks at how we transformed from audience members to computer users to citizen-users, starting with the launch of Microsoft's Windows 95. While widely associated with office drudgery now, Microsoft broke onto the scene more than twenty years ago with a revolutionary suite of tools that radically transformed what was possible for the average computer user with no technical knowledge: the ability to navigate a computer (via Windows) and get work done (via Office), thus contributing to the information-sharing norms in which we operate today. But information-sharing, for some people, is not simply a feature; it's a *right*, something to believe in—and a cause to fight for. And, over the past twenty years, we have become more than simple recipients of

content. We've morphed into something altogether new: citizen-users. Chapter 1 shows how this came to be, how we became citizen-users for whom technology is not just a tool we use but an ideology that dictates how we engage with—and take part in—our governments.

While citizen-users engage with digital content, they're still grounded in a physical landscape. Chapter 2 situates citizen-users in their physical landscape, examining what net states are doing "IRL"—in real life—starting with Tesla's and Google's interventions in Puerto Rico after Hurricane Maria in 2017. It grounds the ethereal internet, "the cloud," in the physical world, tracing how our data is bound to Earth through undersea cables and data centers. The chapter then moves to net state activity in key areas of the physical world. By tracking net state activity IRL, this chapter lays the foundation for a new way of looking at power: distributed not according to borders on a map, but through information flows, investments, and physical assets.

Chapter 3 looks at the battle over our privacy. Privacy is no longer a given. We're engaged in a global battle over who gets to determine the degree of privacy we retain over our content and activities via tech. This chapter explores how our understanding of privacy has evolved and the possibility that its current iteration may be an "anomaly." It also considers how net state partnerships with data brokers create profiles that "know" us, and how some countries are fighting back against these practices. It traces how Europe is leading the way for wielding government regulations over tech companies in defense of citizen-user rights and considers what options Americans have in our currently unregulated landscape.

Chapter 4 considers our physical security, showing how net states like Google became integral to the fight against modern-day enemies. Exploring the differences between the tech ethos and military ethos, this chapter explores how the expertise so prized by the security agencies has become a kind of disadvantage in the fight against terrorism. It shows how net states are uniquely capable of engaging in security issues, through counterterrorism activities via Google's think

tank, Jigsaw. The chapter then shows the possibilities for net state/nation-state cooperation through acts of diplomacy and looks at how net states, led by Microsoft, have begun to forge ahead in this domain.

Chapter 5 examines how we use net state tools to curate idealized versions of ourselves—our profiles and activities online—and how nation-states may enact real-world consequences on what we are or are not permitted to access based on them. Using China's Social Credit Score system as an example, the chapter considers what the networks of connections we create, as well as the carefully managed personas that we upload, say about our needs as individuals, citizens, and citizen-users.

Chapter 6 delves further into our daily life by examining the tech we use in our homes and our public spaces with the Internet of Things (IOT). This chapter explores the ways that the IOT currently influences and is likely to affect our daily existence. It then examines developments in user profiling, starting with Amazon's recommendation systems and "smart" technologies that gather data on our health, our environment, the information we seek, the music we play, and even our sleep habits.

Chapter 7 moves the focus from our actions to our cognition, examining what happens to our minds as we interact with net state technologies. It explores the impact of the uniquely immersive qualities of this tech and how that impacts our thinking, our behaviors, and ultimately, our awareness of ourselves and the world around us. Starting with the most ubiquitous net state tech—the smartphone—this chapter looks at how increasingly immersive properties of our technology affect how we learn, what we remember, and how we perceive the world. From the current tools at our disposal to emerging tech like augmented reality, the chapter considers what an increasingly personalized view of the world might mean for people and societies.

Finally, chapter 8 takes a hard look at where we've been in recent history and where we are now, with staggering rates of depression, addiction, and—unique to America—acts of gun violence. It gives us options for how to reconcile our feelings of empowerment via tech with

our sense of powerlessness in the face of life-altering challenges. This chapter explores what we as citizen-users must do to ensure that we remain actively engaged in the development of net states, their relationship with our nation-states, and how they relate to our own lives, offering a citizen-user pact with net states.

The book concludes with an assessment of how net states have begun to engage with one another and recommendations for governments to join with them or face irrelevance. It argues that citizenship, whether in a nation-state or a net state, requires engagement, and the consequences for failing to engage are dire. In a democracy, failing to vote means losing out on the chance to be represented by those who protect our interests. In net states, failing to engage means losing out on personal privacy, the implications of which are only starting to be understood.

PUBLIC OPINION ABOUT THE ROLE OF TECHNOLOGY IN OUR LIVES SWAYS. In the first 15 years of the new millennium, tech was going to save us all, make the world more democratic, level the playing field, and provide a platform for the disenfranchised to make their voices heard. Then the elections of 2016 hit; Americans were manipulated en masse by Russian misinformation campaigns. Facebook gave 87 million users' data over to the political consulting firm Cambridge Analytica. "Technology addiction" and "Facebook depression" became well-known conditions. Tech suddenly seemed dangerous.

But public opinion on tech will likely swing again. Tech just does too much good for people not to notice eventually. For example, in 2018, in New Delhi, India, a police department instituted a pilot project using experimental facial recognition software. Within four days, more than 3,000 missing children were located.[26] That same year in Australia, two teenage boys caught in rough waters 2,500 feet offshore were rescued when a remote-controlled drone delivered an inflatable rescue pod to the swimmers within 70 seconds of launch. Traversing the same distance would have taken a lifeguard up to six minutes, during which

time the boys could have drowned.[27] And back in the United States, a young woman was warned by her Apple Watch that her heart rate had skyrocketed to 190 beats per minute. This prompted her to get to an emergency room, where she was immediately diagnosed as undergoing what would have been fatal kidney failure.[28]

And so on. Tech can literally save lives. Even beyond its lifesaving capacity, its presence in our daily realm can facilitate better living, with faster answers to our queries, better suggestions for what will be our most beloved book or film, and easier access to aids of all kinds, from maps to encyclopedias, from cookbooks to cameras.

We are not victims here. We've invited tech into our lives for a reason. It makes life easier. It makes life more convenient. Sometimes, it makes life safer. Sometimes, it makes life better. And since tech isn't going anywhere, we owe it to ourselves to know what it *means* that it's here: what our data is worth and how it's used. Just as being a responsible citizen of a nation-state requires paying attention to who's in charge and what they're up to, we need to become responsible citizen-users of our net states, paying attention to who's in charge and what *they're* up to.

Eventually, public opinion will settle somewhere in the middle regarding tech. We will no longer be starry-eyed about its promises or frightened by its possibilities. But until then, we should harness our outrage and our passions to demand that net states take great care with us, their citizen-users. Because while there may be only one Facebook and one Google and one Apple now, those will not always be our only options. Remember, not long ago, there was only one Myspace and one Napster.

Henry David Thoreau once noted, "Is a democracy, such as we know it, the last improvement possible in government? There will never be a really free and enlightened State until the State comes to recognize the individual as a higher and independent power."[29] Net states create tools that elevate the individual, and—just as in our political system—it's up to the individual then to leverage or leave idle that power.

We users have more power over net states than we've yet to claim. *The Information Trade* shows how to be present in the midst of technology, aware of the new ways it controls our world, and able to manage its impact on our lives. We do not need to stop technology from evolving to ensure that it does so responsibly. *The Information Trade* explores what it means to be a responsible citizen-user, engaged with and unafraid of the world that we're building with our tech—and that tech is building for us.