

# THE INFORMATION TRADE

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

ALEXIS WICHOWSKI



**HarperOne**

*An Imprint of HarperCollinsPublishers*



THE INFORMATION TRADE. Copyright © 2020 by Alexis Wichowski. All rights reserved. Printed in the United States of America. No part of this book may be used or reproduced in any manner whatsoever without written permission except in the case of brief quotations embodied in critical articles and reviews. For information, address HarperCollins Publishers, 195 Broadway, New York, NY 10007.

HarperCollins books may be purchased for educational, business, or sales promotional use. For information, please email the Special Markets Department at [SPsales@harpercollins.com](mailto:SPsales@harpercollins.com).

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

# CONTENTS



Introduction 1

## ONE

Rise of the Citizen-User 21

## TWO

Net States IRL 47

## THREE

Privacy Allies and Adversaries 75

## FOUR

Information-Age Warfighters 103

## FIVE

A Great Wall of Watchers 131

## SIX

The All-Knowing Internet of Things 153

## SEVEN

The Mind, Immersed 179

x **CONTENTS**

**EIGHT**

A Declaration of Citizen-User Rights 203

**CONCLUSION**

The Net State Pattern 231

Acknowledgments 245

Appendix 249

Notes 257

## TWO



# NET STATES IRL

**C**itizen-users may engage with digital content, but they're still grounded in a physical landscape. This chapter explores what net states are doing “IRL”—in real life—situating the ethereal internet, “the cloud,” in the physical world and tracing how our data is tethered to Earth through undersea cables and data centers. 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.

Never has Puerto Rico's ambiguous status in the American experience appeared in sharper relief than in the aftermath of Hurricane Maria. From 6:15 a.m. on Wednesday, September 20, 2017, when the category 4 hurricane made landfall in what would be the worst storm the island has ever seen—and the fifth-most-powerful storm to ever hit the United States—the island suddenly seemed to be on its own.<sup>1</sup> The storm ravaged Puerto Rico, battering its 3.4 million residents with winds of 155 miles per hour and more than 30 inches of rain in a single day. As a point of comparison, Hurricane Katrina's rainfall maxed out at nine inches at the height of the storm; its major source of damage came from

floodwaters.<sup>2</sup>

“It was as if a 50- to 60-mile-wide tornado raged across Puerto Rico like a buzz saw,” reported meteorologist Jeff Weber from the National Center for Atmospheric Research. “It’s almost as strong as a hurricane can get in a direct hit.”<sup>3</sup>

Just three weeks earlier, in another part of America, Houston, Texas, had been hit by Hurricane Harvey, an equally powerful storm in its own way. Though less severe in intensity (it had been downgraded to a tropical storm by the time it hit Houston), its rains were relentless, dumping 40 to 60 inches on the 2.3 million residents of America’s fourth-largest city over the course of 117 hours. Harvey flooded 40 percent of the city’s buildings and residences and broke the all-time record for hurricane rainfall in the United States.<sup>4</sup> An estimated 82 people perished in the storm.<sup>5</sup>

The federal government’s response to the flood damage in Texas was swift and massive. The Federal Emergency Management Agency (FEMA) coordinated and deployed over 31,000 personnel from multiple agencies and organizations to the city even before the storm made landfall.<sup>6</sup> President Trump personally toured Houston four days after the storm hit.

To Puerto Rico, with a population double that of Houston, FEMA sent fewer than 500 staffers.<sup>7</sup> The president didn’t appear for almost two weeks. And yet the damage was far more severe than what had befallen Texas. Immediately after landfall, the entire island lost electricity. More than 95 percent of cell service went out. The chief executive of the government-owned Puerto Rico Electric Power Authority, Ricardo Ramos, told CNN, “The island’s power infrastructure had essentially been destroyed.”<sup>8</sup> Hurricane Maria’s death toll from the storm and its aftermath is estimated to be 4,645 people—more than 50 times higher than the loss of life in Texas following Hurricane Harvey.<sup>9</sup>

Time went by. Things got worse. A week after the storm, almost half the population still lacked access to drinking water. Ten days later, that number increased to 55 percent.<sup>10</sup>

Reporters covered the disaster from every angle imaginable—mostly doom and gloom: the loss of life, the dramatic absence of the federal government, the potential looming food shortages, and the consequences of long-term lack of electricity on a population of over 3 million.<sup>11</sup> But one reporter took a different tack, identifying a rare opportunity. At 2:45 p.m. on October 4, 2017, Brian Kahn, a reporter with the environmental news website Earther, filed a story titled, “Puerto Rico Has a Once in a Lifetime Opportunity to Rethink How It Gets Electricity.”<sup>12</sup> A separate tweeter with about 9,000 followers then posted the story with the comment, “Could @elonmusk go in and rebuild #PuertoRico’s electricity system with independent solar & battery systems?”

Elon Musk read that tweet and responded. Given that he has 23.7 million followers, it was rather extraordinary that Musk personally replied to the post. He tweeted, “The Tesla team has done this for many smaller islands around the world, but there is no scalability limit, so it can be done for Puerto Rico too. Such a decision would be in the hands of the PR govt, PUC, any commercial stakeholders and, most importantly, the people of PR.”

Approximately eight hours later, word of Musk’s tweet had reached Puerto Rico’s governor, Ricardo Rosselló. Rosselló tweeted back, “@elonmusk, let’s talk.”

Tech entrepreneur Elon Musk had long made headlines for his almost preternatural ability to plant a flag in future-leaning endeavors. Before most people were even using the internet, Musk cofounded PayPal, an online payment system, in 1998.<sup>13</sup> He designed a proposed “Hyperloop” for high-speed mass transit between San Francisco and Los Angeles, with plans resembling schematics from *Star Trek*.<sup>14</sup> He created SpaceX, which has successfully completed multiple restocking trips to the International Space Station, cornering the rocket launch market.<sup>15</sup> And he formed Tesla, whose electric cars can travel upwards of 400 miles on a single charge.<sup>16</sup> Musk is one of those rare people who can claim to “make life multiplanetary” within his lifetime and be taken seriously.<sup>17</sup>

In 2015, Tesla broke yet more new ground when it plowed into the energy business. It launched Powerwall, a company that makes a rechargeable lithium-ion battery-pack kit—Powerpack—which stores solar power for home owners. The kit can be bought outright (or with loan financing) or leased.<sup>18</sup> “We have this handy fusion reactor in the sky called the sun,” Musk noted at Powerwall’s inaugural press conference.<sup>19</sup> But existing batteries, he noted, “suck.” Powerwall, Musk promised, was going to make traditional batteries obsolete.

In the two years following the Powerwall launch, Musk lobbied hard to get consumers, businesses, and governments alike to adopt solar energy storage via his Powerwall system. He achieved only moderate initial success. In 2015—launch year—Queensland, Australia, which already had one of the world’s highest rates of household solar panel systems (with more than 88,000 such systems) entered into a year-long trial with Powerwall to test how it could integrate Powerwall with the state’s energy infrastructure.<sup>20</sup> Gradually, Powerwall installations began to make gains beyond Queensland and into other territories in Australia, albeit on the consumer rather than the governmental level. In short, despite receiving a positive reception conceptually, Powerwall had yet to really gain a foothold in a large-scale energy grid. Its first big foray into a national public grid was in 2016, when Powerwall provided energy to the entire island of Ta’u in American Samoa. But benefiting a population of fewer than 600 residents, this hardly gave Musk the large-scale proof of concept he craved.<sup>21</sup>

And for Musk, Powerwall wasn’t just some side-job, do-gooder passion project to save the environment. His work on solar energy was part of a larger plan, one that Musk began when he bought the solar energy company SolarCity. During a joint SolarCity-Tesla product launch in 2017, Musk spoke to the crowd of approximately 200 people. “This,” he said, gesturing to solar panels on the roofs of nearby houses, “is the integrated future. You’ve got an electric car, a Powerwall, and a Solar Roof.” As if to shoo away any naysayers in the crowd, he concluded, “It’s pretty straightforward, really.”<sup>22</sup>

With Powerwall, Musk wasn't just launching another business. He was adding to his vision of a future in which energy and transportation would be fundamentally altered from the systems our governments have traditionally relied upon. As noted above, Musk is already transforming transportation: with Tesla (electric cars), the Hyperloop (high-speed urban transit), and SpaceX (space transit). He's transforming energy: with SolarCity (solar panels) and Powerwall (solar energy storage). Combined, these endeavors form puzzle pieces that create an interconnected infrastructure, one that controls how future humans physically will move from place to place and gain access to energy. In so doing, Musk is building a pseudo-public utility. It's not "public," in that government won't own it; Musk will. But these projects in many ways *act* like a public utility, in that they theoretically supply "the public" with basic needs: energy and transportation.

With this backdrop in mind, it makes sense that when Hurricane Maria came along, Musk saw an opportunity, the chance he'd been waiting for to bring Powerwall to scale. Weeks after FEMA's much-criticized response to Puerto Rico's island-wide power outage, Musk stepped up with a tantalizing offer: not only would he donate Powerpack systems to Puerto Rico free of charge, but they could be used as a first step in rebuilding the entire energy infrastructure of the island.

The US federal government—historically responsible, at the bare minimum, for providing basic infrastructure such as power, roads, and water to its people—barely showed up to aid 3 million of its citizens. A tech company—historically responsible for nothing but its bottom line—stepped in with an offer not only to donate equipment but to assume management of the island's energy, an essential piece of critical infrastructure.

Just five days after the Twitter exchange between Elon Musk and Governor Rosselló, Tesla shipped hundreds (no exact number could be confirmed by reporters) of Powerpacks to the island, each of which stores up to 210 kilowatt-hours (kWh).<sup>23</sup> For context, according to the US Energy Information Administration, the average American home uses

about 900 kWh of energy per month.<sup>24</sup> In other words, one Powerpack could provide electricity to one home for about a week—assuming it was never recharged, which, in a sunny environment such as Puerto Rico, was unlikely to be the case.

And Musk's Powerpacks continued to deliver benefits to Puerto Ricans even beyond the immediate aftermath of Hurricane Maria. During an island-wide blackout seven months later, in April 2018, Musk's Powerpack batteries generated electricity at 662 sites across the island.<sup>25</sup> The Powerpacks may not yet have turned into the island-wide energy infrastructure transformation Musk had hoped for. But at the very least, they put themselves on governments' radar.

VERMONT IS PERHAPS THE MOST STRIKING EXAMPLE OF HOW "PUBLIC" infrastructure is being transformed by net states. With just over 600,000 people, Vermont is a small state, population-wise. But it's got a national reputation for punching above its weight when it comes to enacting progressive change. Back in 2000, Vermont was the first state to legalize same-sex marriage—a full eight years before a second state followed suit.<sup>26</sup> As of 2015, Burlington, Vermont, became the first city in the nation to run completely on renewable energy.<sup>27</sup> The state has one of the most technologically advanced energy grids in the country. In 2016, nearly all of its in-state electricity was generated by renewable energy, including hydroelectric, biomass, wind, and solar sources.<sup>28</sup> In fact, the state's campaign to get residents to install renewable energy systems has been so successful that the utility commission recently cut back on awarding financial compensation for doing so.<sup>29</sup> "Renewable energy is flourishing in Vermont," said the commission, "and has reached a level of maturity where it can continue to be deployed with lower incentives."

Perhaps one of the reasons Vermonters take their energy supply so seriously is that they'll quite literally freeze if they don't: with about 81 inches per year, Vermont gets among the highest snowfall of any state in the US.<sup>30</sup> While this may be great for ski slopes, it also means that most

Vermonters have to repeatedly weather winter storms accompanied by extreme cold and winds that down trees and power lines—in fact, this happens an average of once every 13.5 days from October through March. According to the US Department of Energy, power outages affect an average of 69,732 Vermonters each year, roughly 10 percent of the state's population.<sup>31</sup> Some winters are harder than others, of course. In December 2013, for instance, storms dumped 30.7 inches of snow on Burlington, leading to eight power outages that month alone—a black-out once every 3.75 days.<sup>32</sup>

Given these climate conditions, it's probably no surprise that when the energy arm of Elon Musk's Tesla—Powerwall—proposed a pilot home-generator program in Vermont in 2015, utility companies jumped at the chance to participate.<sup>33</sup> By 2017, Vermont's Green Mountain Power offered residents Powerwall backup batteries for \$15 a month for a 10-year contract.

This makes immediate sense for the utility companies: once Powerwall batteries hit 2,000 users, energy use goes down so much that it's like taking 7,500 homes off the electrical grid. It makes sense for homeowners as well. Unlike generators, Powerpacks are integrated into the home energy system.

The advantage for individual users whose homes have solar panels is pretty clear. You pay \$15 a month and get a state-of-the-art backup battery that—unlike a more conventional generator—doesn't require that you remember to gas it up or go out in the snow to get it going. It works to juice up your battery through your solar panels without requiring any activity from you, the user.

And Vermonters aren't the only ones benefiting from this sort of deal: Tesla and its offshoot, SolarCity, have deployed solar arrays and Powerpack systems to the city of Manchester in the UK<sup>34</sup> and, as mentioned, to tens of thousands of homes in Australia,<sup>35</sup> as well as utility companies within several US states. In short, Tesla is edging into what used to be government turf: the electrical grid. In addition to Vermont, Powerpacks are now integrated into the electrical grids in parts of Ha-

waii,<sup>36</sup> Colorado,<sup>37</sup> New York,<sup>38</sup> California, and Connecticut<sup>39</sup>—Tesla is now responsible for providing the infrastructure to light and heat the homes of over 2 million American citizens. The question is whether those citizens are aware of this.

Again, as with the response in Puerto Rico, chances are that so long as the lights stay on and the house is a comfortable temperature, people won't give much thought to who's providing the energy to their homes. Yet, as with Puerto Ricans, it would benefit Vermonters and residents of other states to remain vigilant about the fact that their "public" infrastructure—their energy grid—may not be in fact be publicly owned and operated, but rather outsourced to a tech company.

A short time after Tesla showed up after Hurricane Maria in Puerto Rico, Google came, too. Google (or rather, its parent company, Alphabet) has also been developing numerous infrastructure-related projects in recent years—notably, Project Loon. Launched in 2013, Project Loon emerged with a veritable army of what look like hot-air balloons intended to be deployed in the stratosphere around the globe. The goal: provide free high-speed internet access to rural and remote areas—or, as Project Loon's tagline says, "Balloon-powered internet for everyone."<sup>40</sup> Since Project Loon launched its first balloons, it has partnered with governments in Brazil, France, Sri Lanka, and Indonesia. Successful as the partnerships have been, though, Google continues to label them "tests."

Hurricane Maria offered Google a new opportunity: the chance to supply telecommunications and internet—not as a pilot program or an add-on service, but as part of the critical infrastructure to an entire region. Less than a month after the hurricane hit, Project Loon filed an application with the Federal Communications Commission to partner with the local telecommunications provider, AT&T, to deploy its balloons.<sup>41</sup> The application was cleared the same day. Cynically, one might see this as the federal government's eagerness to get rid of the responsibility for providing relief to Puerto Rico. But Federal Communications Commission chair Ajit Pai insisted the decision was simply pragmatic. "More than two weeks after Hurricane Maria struck, millions of Puerto

Ricans are still without access to much-needed communications services,” he said. “That’s why we need to take innovative approaches to help restore connectivity on the island.”<sup>42</sup>

Just eight months after the hurricane, Project Loon and AT&T had indeed restored connectivity, with cell service and internet connections to the majority of the island.<sup>43</sup>

Again, the residents of Puerto Rico probably didn’t care who fixed their electrical grid or got their cell phones working. Chances are, they were just glad they worked. With the infrastructure problems sorted, at least for now, it would be tempting to move on without considering the intentions or implications of the whos or hows or whys of it all.

But if people had the luxury of stopping to think about what transpired here, they might note that the infrastructure fixers were not governments, but rather tech companies. This matters. While net states acted in this instance the way we’ve come to expect governments to act, they differ from governments in two key ways. First, unlike governments, net states are under no legal obligation to maintain in perpetuity the infrastructure they implement. The Powerwalls and Project Loon in Puerto Rico may have been just another pilot project for Tesla and Google: one that could morph into a permanent program, or one that they draw to a close as soon as they’ve amassed the data they’re looking to acquire. Second, while net states do engage in contracts for services, they are not mandated by law to assist any other states or territories that should find their energy and telecom infrastructures wiped out by storms in the future. In other words, net state activities in Puerto Rico don’t set a precedent for net state responsibilities in the future.

The result of these two key differences is that net state-sponsored aid may not last, or even be offered in the first place, regardless of the needs of the people. Project Loon’s CEO, Alastair Westgarth, wrote in a blog post that Google would keep the Loon balloons flying over Puerto Rico “as long as it is useful and we’re able to do so.”<sup>44</sup> It’s hard to imagine a contract between citizens and a public utility company like Con Edison or AT&T either (1) providing free internet or cell phone services

at all, or (2) pledging to continue to provide such services for a period of time as vague as “as long as we’re able to do so.”

This statement is a reminder that just because net states offer infrastructure services doesn’t mean they’ll *always* offer them. And because they’re free, we, as consumers, don’t get a say in how long net states will continue to provide these services or under what conditions. In Puerto Rico, Tesla’s and Google’s offerings have not been infrastructure as a public good, but infrastructure as charity; an endowment by net state to consumer, granted or removed as and when net states see fit.

PROJECT LOON’S 50-FOOT-WIDE BALLOONS AND TESLA’S SHED-SIZE Powerpacks serve as useful reminders that even invisible resources—in this case, internet access and energy—originate from something physical. This holds true with other invisible resources as well—most notably, our data.

Ninety-nine percent of our data is transmitted online through 428 undersea cables that collectively stretch 700,000 miles—enough to circle Earth 28 times. (There are also underground cables—542 in the US alone—but undersea cables manage over 95 percent of the total global data traffic.)<sup>45</sup> The fiber-optic cables are thin, roughly the diameter of a garden hose.<sup>46</sup> As technology reporter Jameson Zimmer aptly put it, “The Internet is commonly described as a cloud. In reality, it’s a series of wet, fragile tubes.”

It’s not surprising, then, that the cables are vulnerable to physical damage from any number of things. In 2008, off the coast of Dubai, an errant ship cut off internet service for 75 million people in Europe and the Middle East.<sup>47</sup> An earthquake off the coast of Taiwan in 2006 knocked out connectivity for most of Southeast Asia.<sup>48</sup> Amazingly, sharks are a problem as well—they apparently have a real taste for fiber optics. By 2014, so many sharks were biting through Google’s underwater network that the company started wrapping its trans-Pacific cables in Kevlar.<sup>49</sup>

Internet cables are sort of the plumbing of technology. When they

work, we rarely think about them, no more than we think about how water runs through our pipes when we turn on our kitchen faucet. When we're watching YouTube, if a video loads it's easy to ignore *how* data is transmitted through the many data centers, servers, and under-sea cables that bring internet-enabled content to our device.

As it turns out, the plumbing matters quite a bit when we're talking about data. Entertainment may not be the noblest reason to care about it, but for many people, it's certainly one of the most relevant. Americans work pretty hard: full-time-employed adults put in an average of 47 hours a week, almost six full workdays.<sup>50</sup> Factor in an average of 14 hours a week actively parenting<sup>51</sup> and 12.67 hours of cooking, cleaning, laundry, and other household chores, and this adds up to more than 73 hours of work, paid and unpaid, per week. There's little time left for leisure, but by cutting out sleep—as a nation, we're down to around seven hours a night<sup>52</sup>—we manage to find two to four hours per day to escape reality: notably, by watching TV.<sup>53</sup>

From personal entertainment to professional communications, net states are the mediators of our attention, at work and at home. They produce the devices that we use to go online—our iPhones and our laptops and our internet-enabled televisions—as well as the platforms on which we spend our time online: watching videos on Google-owned YouTube, reading the news on social media sites like Facebook, or getting work done via productivity packages such as Microsoft Office.

Given that net states supply our online destinations and the devices to get us there, it's not surprising that they are increasingly interested in controlling our *means* of access as well: the physical cables that provide internet access and the data centers that store our data. The cables matter because they're how we stream data. And we use a lot of it: 190 gigabytes per month for the average American household.<sup>54</sup> Twenty hours a month on Facebook alone consumes approximately 2.5 gigabytes of data.<sup>55</sup> Net states want more control over ensuring that your data actually gets to you. Until recently, Google, Facebook, Amazon, and other net states leased bandwidth from telecommunications companies that

owned undersea cables.<sup>56</sup> But starting in 2016, net states started buying the cables themselves, either in whole or in part, to ensure that they retain greater control over the cables' maintenance, usage, and upkeep: by the end of 2017, Amazon owned or co-owned two cables; Microsoft, four; Facebook, eight; and Google, fourteen.<sup>57</sup>

That may not sound like much considering that, as noted earlier, there are more than 420 undersea cables all told. However, the significance lies not in the net total; it's in the pattern. Three years ago, net states owned zero cables. Now, in 2019, Google alone owns or co-owns 63,605 miles of cabling—about 8.5 percent of the total length of all undersea cables—enough to wrap around the earth's equator two and a half times and still have cable to spare.<sup>58</sup> To go from owning zero miles of undersea cabling to just under 64,000 miles in just three years is an astonishing growth rate, and one that begs the question: Why?

The answer is simple: the cloud. With net states more involved in being cloud service providers in some shape or form, controlling the *means* of data transmission moves from being a simple technical convenience to an absolute business imperative. Because the more that net states and their services push data to and from the cloud, the more we as users gobble up bandwidth. From 2016 to 2017, data flowing through the cable network increased 52 percent. Globally, we transmitted 689 terabytes of data every second. So the more cables that net states can own themselves, the more opportunities they acquire to expand from simply providing digital services to controlling how fast we can get the *content* moving in and out of those services.

The cloud, where this content is increasingly stored, is, like the internet, also physically bound to Earth. While the very name “the cloud” suggests that data is something intangible, a swarm of electrostatic bits drifting in the air somewhere, our cloud-based data is still located in a storage center in a physical location somewhere, in some country. Google's cloud platform, for example, operates caches at 90 data centers in North America, South America, Europe, Asia, and Australia.<sup>59</sup>

The cloud's physical footprint serves as a reminder that while net

states may be headquartered in one country, they operate internationally—in terms not only of who uses their products and services but also of who houses their infrastructure. We may not know whether our data is stored in Europe, which now has the most stringent user data protection laws in the world, or in Taiwan, whose laws are far less strict. But it's handy to keep in mind that when we send an email or store a document in the cloud, this data is, in fact, stored somewhere, physically, in the world. What's more, the laws of the country or countries in which the data is stored, sent, or received may factor into who ultimately has access to it. And as of this writing, net states are by far the most influential parties in making that determination.

All of these various activities combine to reveal a pattern: net states are migrating from the digital to the physical, easing their way into our everyday experiences through the energy grid that powers our cities, the communications satellites that facilitate net use, the food services we rely on, and the healthcare industry that manages our physical well-being. While governments may still serve as the primary holders of public infrastructure, they're facing increasing competition from net states that want to be part of the “boring” yet powerful scaffolding that orders our lives—and collects valuable data about us while they're at it. (More on why that data matters in chapter 3.)

Consider just one particular sector: health. In November 2018, Google hired the CEO of a healthcare system, Dr. David Feinberg, to manage its move into the health business.<sup>60</sup> His mandate is to consolidate strategy and operations across various Google health-related initiatives, including its search engine, its cloud storage business, the Google Brain artificial intelligence program (just a slice of folks working on AI at Google), Nest (owned by Google), and Google Fit wearables. Of particular interest to citizens are the possibilities that emerge when combining the personal data collected across these groups.

For instance, with Google Fit, Google captures your physical health data, such as heart rate, blood pressure, activity frequency, and physical routes traversed.<sup>61</sup> With Nest's suite of products, they track your move-

ments outside and inside your house, not only via Nest security cameras that you've installed but also via motion-detecting sensors in your smart appliances—anything connected to the internet—such as, potentially, your thermostat, fridge, coffee maker, television, and anything else you've connected to the web.<sup>62</sup>

Google's search engine already customizes your search results based on prior searches, the content of your emails (if you're on Gmail), and your web-based activities. With the health data it can now acquire through Fit and Nest, Google can customize your search results even further, adding in not only the questions you ask *about* your health—like, “What are common flu symptoms?” and “Which are the best running routes near me?”—but your *actual* health. Because it now has data beyond what you report. It has the data that it observes: information about your bodily functions, like your heartbeats and breaths per minute; your activities, like how often you open the fridge; and your movements, like when you leave the house, where you go, and when you come home again. Compiled, Google's health programs act like a personal private investigator on your tail, tracking your actions both indoors and out. Google and net states like it are no longer limited to a person's online activities. With smart home products and wearables, they're asserting a presence into people's physical lives, a new market they're only beginning to explore.

DESPITE GOOGLE'S AND TESLA'S ADVANCES INTO PUBLIC INFRASTRUCTURE projects—which used to be the sole domain of governments—they're clearly not governments, let alone countries or, to use the wonky term for such entities (as I have several times thus far in this book), “nation-states.” Outside policy circles, “nation-state” is not a term you run into often. In some ways, it's just a fancy word for “country.” But there's a bit more to it. Nation-states are defined by three key components: First, they have a physical territory with distinct borders. Second, they have a “people”—individuals and communities bound together by an overarching culture, which may include several ethnicities and subcul-

tures. Third, they have a government—a body that provides communal utilities (things such as roads, bridges, and power systems), protection from harm (whether from other citizens or from foreign actors), public services such as access to education, and some sort of financial system.<sup>63</sup>

No matter what country—what nation-state—we live in, it's easy to take for granted that governments actually provide these things for us. For instance, I can't remember the last time I reflected in the moment on how lucky I was to be driving on a paved road rather than a dirt one. Even in developed countries, there remain millions of miles of unpaved roads. (Fun fact: the United States still has 1,417,903 miles of dirt roads that compose 34 percent of all American roadways.)<sup>64</sup> As for these kinds of background services—roads, bridges, military protection, a functional banking system—it's probably a good sign if you *don't* notice them. As *New York Times* columnist David Brooks once wrote, "Government is essential, but . . . it's the stem of the flower, not the bloom. The best government is boring, gradual and orderly."<sup>65</sup>

Net states operate similarly: in the background. Digital platforms are stems. Both in digital and in physical life, the bloom is people, living their lives. The bloom is the actions, interactions, thoughts, hopes, worries, and silliness of us all. The stem, to use Brooks's metaphor, *enables* life, but it's the people who flower.

Net states get this. They are always and forever trying to get people to use their services to create and recreate life in digital form: to post updates about their day, share stories they found interesting or funny or weird or annoying, or upload visceral images that capture the feel of a moment, a day, a creature, or a tragedy. Net states, like nation-states, are background: they provide the foundation for our online communities, the space for a people to come together. They also provide the services that make our interactions—our online lives—possible. In these ways, what net states give us—services that enable some portion of the goings-on of life—is not so very different from what nation-states provide for us.

However, there is a point where the similarities between net states and nation-states end and the two sorts of entities become very differ-

ent in important ways. While we may be *of* the digital world, we still reside *in* the physical one. In other words, so long as we have bodies, we need to park them somewhere. And, while net states permit us to connect with like-minded people—*our* people, a community that shares our culture and values and beliefs—across the globe, in places like Niger and Peru and Afghanistan and Brazil, each of us is subject to a very different physical existence precisely because of where our body is parked. No amount of sharing of beliefs or values or culture can change the differences in our lived, physical experience. For instance, net states can't change that a like-minded friend in Niger will experience a power outage an average of 22 times a month (if they even have electricity at home in the first place). Living in Brooklyn, I almost never worry about this happening.<sup>66</sup> Net states also can't do anything about the fact that a like-minded friend living in Afghanistan is 87 times more likely to be harmed in a terrorist attack than another friend who lives in Brazil.<sup>67</sup>

Or can they? What happens when net states enter terrain formerly the primary domain of nation-states?

IN 1943, ABRAHAM MASLOW FAMOUSLY POSITED THAT HUMANS UNIVERSALLY long to fulfill a hierarchy of needs. Using a pyramid to illustrate his point, Maslow showed how humans must first meet our physical needs—food, water, warmth, and shelter—before we can move up the hierarchy to our emotional-social needs, such as interpersonal connection. Finally, at the top of the pyramid come self-fulfillment and creative needs: what he termed “self-actualization.”

Skip ahead to the information age. Tech companies and collectives started out solely focused on the tip of the pyramid, enabling users to find, manipulate, store, share, and otherwise wield information that would help us reach self-fulfillment. Base-order needs such as food, water, warmth, and rest were left to governments to address.

Until recently, that is. Net states have quietly been moving down the pyramid. Entities like Facebook and Twitter, for instance, have long

dominated the middle, allowing people to connect and fulfill their need for belonging and even, perhaps, their need for emotional connection. Increasingly, they're moving farther down the pyramid toward our most basic needs: Amazon recently entered the food business with its purchase of Whole Foods. Elon Musk's Powerwall marks his flag-staking in the energy storage business. Net states of all kinds are funding projects that will directly harvest natural resources. And so, while tech dominated the top of our hierarchy of needs when we entered the information age, they're increasingly investing in and seeking to control aspects involving our base needs as well: things like food, shelter, and warmth—areas that historically have sat squarely in the wheelhouse of the nation-state.

Take infrastructure, such as Google's and Tesla's forays into hurricane-ravaged Puerto Rico, two of the most high-profile examples of tech's increasing investment in IRL domains. To confirm that these ventures weren't just anomalies, I decided that I needed to understand more about what net states are up to. That required looking beyond the stories here and there and relying on a more systematic assessment. As the saying goes, I followed the money.

In May 2018, I examined every single acquisition and investment made by the most influential net states—Apple, Google, Microsoft, Tesla, Twitter, and Amazon—over the past 20 years, from the earliest available data in 1998 to May 16, 2018.<sup>68</sup> Using publicly available transaction data from Crunchbase, the premier tech industry database, I came up with a total of 1,227 investments and acquisitions.<sup>69</sup> Next, I identified which of these investments and acquisitions seemed like distinct departures from online-focused activities—that is, that dealt specifically with goings-on in the physical world. This included investing in and buying companies working on the energy grid, on public transportation systems, on agriculture and food markets, on medicine and healthcare, on the telecommunications infrastructure, and so on. (See this book's appendix for a complete list of sectors and companies.)

Of the 1,227 companies the six net states invested in or acquired over the 20-year period, 232 met the criteria for physical-world activities. Put

another way, of all the money Big Tech spent from the late 1990s to 2018, almost 20 percent went to products, services, and activities focused on the physical world.

The primary areas where net states put their money in physical sectors are shown in table 2.1, with those sectors broken into more specific categories in figure 2.1.

| SECTOR                            | # OF INVESTMENTS / ACQUISITIONS | % OF NONCORE TECH ACTIVITY (N=232) |
|-----------------------------------|---------------------------------|------------------------------------|
| Health & wellness                 | 51                              | 22%                                |
| Biotechnology                     | 29                              | 12%                                |
| Energy supply & grid              | 21                              | 9%                                 |
| Telecommunications infrastructure | 21                              | 9%                                 |
| Manufacturing                     | 16                              | 7%                                 |
| Agriculture & food markets        | 16                              | 7%                                 |

TABLE 2.1. Net State Investments & Acquisitions in Physical Sectors, 1998–2018

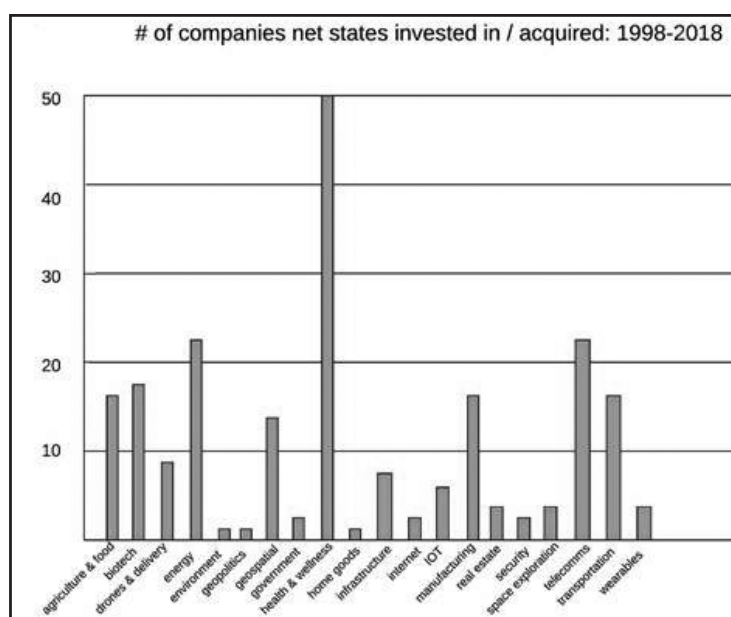


FIGURE 2.1. Net States Investments & Acquisitions, 1998–2018, by Category

The six most influential tech companies in history—Microsoft, Apple, Google, Tesla, Amazon, and Twitter—spent nearly 20 percent of their money buying or investing in products, services, and activities that exist offline, firmly rooted in the physical world. Google invested in entities such as Impossible Foods, a company dedicated to developing organic “meats and cheeses” derived entirely from plants. Facebook bought Endaga, a company that creates telecommunications-in-a-box devices, while Google cofounder Larry Page bought Kitty Hawk, a flying car company. While this was Page’s personal purchase, not a Google investment, the activities of the net state founders—Page and Brin for Google, Musk for Tesla/SolarCity, Bezos for Amazon, and so on—often illuminate the kind of future tech their companies then adopt. For instance, in 2008 Jeff Bezos purchased Rethink Robotics, described as “a leader in collaborative robotics, specializing in ... robots that can work alongside humans.”<sup>70</sup> Four years later, Bezos’s company Amazon bought Kiva Systems (renamed to Amazon Robotics), whose specialization is robotic fulfillment systems in Amazon warehouses, working alongside human operators. For this reason, for this analysis I included the investment and acquisitions activities of the net states themselves as well as those of their research arms (for example, Google X), subsidiaries (for example, Elon Musk’s SolarCity), venture capital funds (for example, GV, an entity of Alphabet, Google’s parent company), and founders (for example, Mark Zuckerberg).

These purchases reveal a pattern: net states are quickly expanding from the online to the world in real life, and not just conceptually: they’re doing so through substantial financial investments. In addition to shaping our digital experiences, net states are building their ability to shape our real-life experiences as well—and they’re willing to bet nearly 20 percent of their acquisition and investment dollars that they can.

With 232 investments and acquisitions composing the data pool in question, there are simply too many variables to permit sweeping claims about why. It’s not immediately clear, for instance, why Amazon

bought the organic food chain Whole Foods in 2017, or why Facebook put money into Ocean's Halo, a seaweed-processing food outfit, or what Google was really going for when it bought the wind-turbine company Makani Power in 2013. There are likely excellent business reasons for all 232 physical world industries that meet some primary need, including infrastructure, health, and food. For example, Facebook most likely invested in telecommunications infrastructure to ensure that more people can go online to use Facebook. Amazon probably fed money into drone delivery to ensure that people continue to buy their wares from Amazon. There are surely sound bottom-line reasons for their investments.

Yet I suspect there's more to the story, for two reasons. First, think of the scale. It makes sense that tech companies would spend the majority of their acquisition and investment dollars—80 percent, as it turns out—on their core technologies: better geolocation services for Google Maps, for instance, or software that facilitates faster processing for Microsoft. It would also make sense that tech companies in particular—organizations that found success precisely because of a future-leaning innovative bent—would spend at least a little money on research and development of new technologies to nudge them along.

But close to 20 percent of their total investment and acquisition funds is more than a *little* money. It represents *billions* of dollars. The single transaction to purchase Whole Foods cost Amazon \$13 billion, a heck of a lot of money to spend on something just because it's shiny and new, even if it probably benefits your bottom line.

The second reason has to do with the changing nature of digital technology. With the advent of the smartphone in 2007, we went from going online on a desktop or laptop to carrying the internet on our person. "Online" is no longer wholly distinct from "in real life"; it's integrated *into* real life. It makes sense, then, for the keepers of our digital lives to branch into our physical and personal spaces. If nothing else, doing so means they have more control over when and how their products and services will be put to use.

Thus, while net states are still largely digital beasts, through expan-

sion into the daily activities of our physical environments, they are becoming, slowly but surely, more closely tethered to the physical world.

Before they can expand much further into our physical environments, however, they need to shore up the supply of material resources required to produce, operate, and maintain the core products and services they already manage within the digital realm. To do so, they've had to be creative. They're not just exploring new sources for traditional resources, such as mining for tantalum—a mineral used in the building of cell phones—in the politically fraught Democratic Republic of Congo. Nor are they settling for access to the abundant mineral reserves in northwestern China. They're also looking to outer space.

In 2012, Google's former CEO Eric Schmidt and cofounder Larry Page became principal investors in an asteroid mining company called Planetary Resources. Asteroid mining may seem like far-flung future tech—and, at present, it may still be—but it's also one of the fastest-growing space-related investment areas out there. Peter Diamandis, cofounder of the X Prize, likened asteroid mining to the next “gold rush,” with space rocks supplying a potentially limitless supply of rare earth metals essential to modern consumer electronics, including everyday items like your laptop and cell phone.<sup>71</sup> The 17 elements classified as “rare earth metals”—from the lithium in your iPhone battery, to scandium, essential for televisions and digital screens, and neodymium, an integral part of your headphones—are currently harvested from Earth's crust.<sup>72</sup> However, like most precious natural resources, they're expensive to mine and process, and at some point risk scarcity in supply.<sup>73</sup>

Elon Musk is also in on the space game, but for other reasons: inter-space travel. In another testament to his prescience, Musk founded the spacecraft manufacturing and ferrying service SpaceX in 2002, more than a decade before other private-sector entities began investing in space. Despite multiple failed launch attempts in its early years, SpaceX has finally hit its stride: in 2017, it successfully launched its first fully recycled mission to the International Space Station, using previously flown rockets and spacecraft for the mission. Since then, it has advanced

so rapidly that analysts estimate SpaceX now controls 50 percent of the rocket launch market globally, a share so substantial that Russia's chief space-flight official, Deputy Prime Minister Dmitry Rogozin, conceded in a recent interview with Russian television that it "isn't worth the effort [for Russia] to try to elbow Musk . . . aside."<sup>74</sup>

Space exploration has historically been so expensive, so specialized, that no commercial entities had either the capital or the technical expertise to try it. Historically, only countries could harness the resources to pull it off. This looked like it might change in 1982, when Space Services' *Conestoga 1* made history as the first privately funded spacecraft to perform a test launch that reached space.<sup>75</sup> Despite this effort, for the next 30 years spacefaring remained primarily the domain of countries.

Even for entities as rich in resources as nations, outer space is a reach. Since the early days of the space race, only nine countries—the United States, Russia, China, France, the United Kingdom, India, Israel, Iran, and North Korea—have developed the capacity to launch anything into orbit. About 60 countries maintain satellites in space,<sup>76</sup> but they have to hitch them to a spacecraft from one of the nine spacefaring nations to get them there. In short, until relatively recently, the only robust investments into rocket launchers, spacecraft, and other orbitals were restricted to deep-pocketed superpower nation-states: Europe, Russia, the United States, and, most recently, China.

In recent years, SpaceX, with its innovative rocketry, has dominated the commercial market. No other private spacefaring company has successfully recycled rockets, a feat that revolutionizes the possibility of reducing the cost of space travel. And yet, being the sole entity currently capable of executing this feat, SpaceX recently raised the ticket price to NASA for restocking the International Space Station—a sobering example of what might happen if governments continue outsourcing space exploration to the private sector.<sup>77</sup>

And Musk likely won't be alone in dominating space for long. In 2018, Amazon founder and CEO Jeff Bezos announced that he's investing \$1 billion a year of his own Amazon stock in his company Blue

Origin, with claims that they would be transporting tourists to the edge of space by 2019.<sup>78</sup>

Asteroid mining and the new race into space are reminders that the material resources that create our tech world are not a given. The electronics that we rely on and take for granted—our cell phones, laptops, tablets, watches, televisions, and the like—are not magically produced out of thin air. We've become used to their being built at the rates they are today, and to their getting faster and generally cheaper with each passing year,<sup>79</sup> but these historic norms are not assured in the future, nor is the very existence of the devices themselves—not by any stretch of the imagination. These gadgets require physical resources, on Earth or from space, that are far from easy to harvest.

Similarly, the investment by net state leadership from Microsoft, Google, Amazon, and SpaceX suggests that outer space is not merely an interesting new frontier to explore. Rather, it is likely essential for the continued dominance of net states. That investment may indicate that conditions on Earth aren't quite as hospitable for expanded business opportunities as we have thought. It also may explain why net states are expanding their businesses from the purely digital into the physical realm—into areas where they might not be quite so reliant on precious minerals from a single country, and an authoritarian one at that.

Because, as of today, between 90 and 95 percent of processed rare earth metals come from land owned by China.<sup>80</sup> The US, for instance, gets the vast majority of these materials from the Chinese, a fact that likely makes the Department of Defense, which itself consumes 800 tons of rare earth metals each year, rather nervous.<sup>81</sup> While the US has its own rare earth minerals reserves, they're barely mined at all: as of May 2019, there was only one rare earth minerals mine in operation, in Mountain Pass, California.<sup>82</sup> China's overwhelming monopoly on Earth-sourced rare earth metals is so valuable that they've created a shipping port in landlocked Kazakhstan—a shipping port so far from the sea that it's practically sitting on the Eurasian “Pole of Inaccessibility,” the official term for the most remote regions on Earth.<sup>83</sup> It's part of China's

planned global “New Silk Road” trading route, hailed by Chinese president Xi Jinping as “the Project of the Century.” Also known as the “Belt and Road Initiative” (formerly “One Belt, One Road”), BRI involves ports, train routes, pipelines, and other infrastructure throughout 70 countries.<sup>84</sup> Through these routes they’re selling all manner of goods, key among them being their processed rare earth metals.<sup>85</sup> China has already invested over a trillion dollars in its infrastructure.<sup>86</sup>

With China processing upwards of 90 percent of all rare earth metals and constructing the largest shipping route in history, the tech industry’s ability to produce digital devices would be absolutely decimated should China decide not to sell these resources to Western net states. With so much of the necessary raw material needed for tech in the control of a single country, the idea of net state entrepreneurs investing in asteroid mining suddenly doesn’t seem so crazy after all.

Here’s the final reason why asteroids and the new space race matter: net state investments and activities may feel academic and distant, but behind the scenes they’re exploratory moonshots, literally—projects so grand that they would take us into space, onto asteroids, and who knows where else. We may think of net states as benign but cool—making search engines, social networking sites, and smartphones. But they’re doing so much more than this. They are seeking to transform our experience on Earth and, in a handful of years, above it.

“THE WORLD IS MUCH BETTER. THE WORLD IS AWFUL. THE WORLD CAN be much better.”<sup>87</sup> Max Roser, an economist at Oxford University, wrote this headline to a blog post explaining how the content of his online publication, *Our World in Data*, can be construed. “All three of these statements are true,” he wrote. But he countered that while “it is important that we know what is wrong with the world[,] . . . given the scale of what we have achieved already and what is possible for the future, I think it’s irresponsible to only report on how dreadful our situation is.”

Roser’s publication tracks long arcs—historical trends over

centuries—about the most important questions in life: How do our lives today compare to those of people who lived four hundred years ago? One hundred years ago? Fifteen years ago? He uses statistical data to tackle dozens of variations on this question. Are we living longer? Are we fighting less? Are our children stronger? Are we suffering less?

And the answer to all of these—*all* of these—is that yes, over long periods of time, life has improved. We are living longer. We are fighting less. Our children are stronger. We are suffering less.

But we still have so much work to do. Our progress hasn't traced a straight line from bad to better. Nor has good fortune been evenly distributed across the globe.

It's sometimes tempting to see today's technology as somehow qualitatively different from previous epochs of tech; its transformation of our experience on Earth as a wholly new, and often bad, thing. Yet "modern" technology has been in the process of transforming our experience on Earth for over a hundred years, since long before net states came to be. With the widespread adoption of radio in the 1920s, for example, we could hear human voices from across the world, and with that new experience, expand our ability to humanize those with different lives than our own. With the mass distribution of television in the 1940s and '50s, we could see human faces across the world, and with that, grow in our capacity to empathize with hardships lived by others.

In some ways, net states have made our world better. In others, they have made our world awful. And in yet others, they have the capacity to make our world *much* better in the years to come. The first Powerpacks Musk took to Puerto Rico less than two weeks after Hurricane Maria had wiped out power to over 3 million residents were delivered to a San Juan children's hospital, Hospital del Niño,<sup>88</sup> a central medical facility that served over 3,000 children and housed more than 30 seriously ill children who required round-the-clock care. One could cynically argue that Tesla helped out just for good publicity, which they certainly got in spades. But regardless of their motivation, they made things happen at a time when the people's own government was failing them. "I've never

seen a team arrive so fast and work so fast. They built this in a week,” Rafael Pagán, the hospital’s chairman of the board, said to Telemundo.<sup>89</sup> Compare Tesla’s activities those weeks to the American government’s; not many days before Tesla’s donation, the American president threw paper towels to a crowd assembled at a press conference. Paper towels. Between net states and the nation-state, it’s not hard to see who really made a difference to the people of Puerto Rico in this instance.

Tech moves fast; it evolves at dizzying speeds. But it’s still trackable and traceable over time. In another few decades, we will have the luxury of looking back at net states’ longer arc of progress or decay, their contributions to or degradation of humanity. But even with the data we have thus far, I would argue that the trend points toward progress. The question then becomes, What is *our* role, as citizen-users? With government, our role as citizens is clear: we vote; we support or oppose laws; we ensure that our peers receive a fair trial when called upon to do so.

But with net states, our role is not only less clear; in some ways, it doesn’t yet exist. Thus far, we’ve yet to vote for their leadership. We’ve yet to assert our personal values on their data and product policies. We’ve not substantially swayed their investment decisions. Throughout this book I argue that we have a responsibility to change all that; that unless we demand a more active, contributory role in net states’ use of our data and their investments in what has been, up to now, *public* infrastructure, we will miss out on the opportunity to shape how they influence our lives: socially, politically, and even physically.

Net states’ expansion into real life is not on the horizon; it’s underway. This could make life better. It could make life awful. Both of those statements may end up being true to some degree, depending on how you look at things. But what is absolutely true, regardless of the vantage point, is that tech in our lives *could* be much better if it included our active participation, both in guiding how it integrates into our real lives and in having a say about what happens with the data this integration generates.

As Roser concludes in his post, “We know that it is possible to make

the world a better place because we already did it. It is because the world is terrible still that it's so important to write about how the world became a better place." For us, it's possible to see how tech has made our real lives better. And it's possible to imagine how it could make our real lives unbearable. Our job is to pay attention; not just to the content our net states produce—the TV shows and the memes and the headlines—but to the net states themselves. We're their citizen-users and their product consumers and their watchdogs, all at once. Playing all three roles is a lot of work. But the consequences of ignoring any one of those roles would be worse. We need to evolve, ourselves, from consumers and passive users of net state resources to active participants—to grow out of our passive role as users and step into an active role as citizen-users.



## THREE



# PRIVACY ALLIES AND ADVERSARIES

Privacy is no longer a given. We personally, and regulators on our behalf, are 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 considers how net states’ partnerships with data brokers create profiles that “know” us, how Europe is fighting back against these practices, and how these interventions can and can’t help the citizen-user.

On August 17, 2018, for the cost of a \$400 court filing fee and undisclosed legal expenses, Napoleon Patacsil, a San Diego–based security guard at CSE Security Services, filed in California’s Northern District Court a class-action lawsuit on behalf of all US users of Android phones and iPhones against Google.<sup>1</sup> *Patacsil v. Google, Inc.* argued that Google illegally tracked users’ locations, regardless of user privacy settings, and without adequate disclosure.<sup>2</sup>

Patacsil leaped to action after reading an Associated Press report just days earlier unmasking Google’s location-tracking practices. The AP report, which was corroborated by researchers at Princeton University,

ran with a detailed map of all the places postdoctoral researcher Gunes Acar had visited over three days in July while his phone's location-tracking capability was turned off. Jarring in detail, the map is accurate down to Acar's presence at specific buildings on a city block.<sup>3</sup>

Patacsil himself, despite mounting a court case to take down one of the most powerful web companies on earth, remains an almost invisible entity online; he granted no interviews regarding his motivations to sue Google. The only details that can be gleaned about his intentions come from the official August 17 court filing itself. It notes that Patacsil owned an iPhone from 2016 through 2018 and had attempted to turn location-tracking services by Google off on this device. "Nevertheless," reads the filing, "Google continued to track his location information." Despite Google's public assurances that turning off location-tracking means that "the places you go are no longer stored"—that "when you turn off Location History for your Google Account, it's off for all devices associated with that Google Account"—the filing characterized Google's representations as "false." Citing the AP report, the filing reads, "Turning off 'Location History' only stopped Google from creating a location timeline that the *user* could view. Google, however, continues to track the phone owners and keep a record of their locations."

Immediately after the Associated Press exposé, Google changed the language in its terms of service to read, "Some location data may be saved as part of your activity on other services, like Search and Maps." Privacy advocates weren't impressed with Google's update. The damage to users—unknowingly having their data location tracked and stored for, potentially, years—had been done. As Princeton computer scientist and former chief technologist for the enforcement bureau of the Federal Communications Commission, Jonathan Mayer, was quoted as saying in Patacsil's court filing: "If you're going to allow users to turn off something called 'Location History,' then all the places where you maintain location history should be turned off. That seems like a pretty straightforward position to have."<sup>4</sup>

Perhaps most significantly, Patacsil is one of only 39 million people—

the residents of California—out of the 325 million people who live in the United States who is even capable of filing a lawsuit against Google, or any other tech company, and having any hope of winning. That's because his home state of California had adopted, a month before Patacsil's filing, the California Consumer Privacy Act of 2018, or AB 375,<sup>5</sup> the most stringent data protection law in the country. Though it won't take effect until January 2020, the spirit of the law and the increasing demand for the regulation of net states emboldened Patacsil to file his class-action suit. Outside the state of California, however, there are currently no other laws on the state or federal level in the US substantially regulating what net states like Google or Facebook can and cannot do with a person's digital information. Nor are there any laws preventing third-party data brokers from collecting, cataloging, and selling our personal, medical, and financial information. Americans—outside the state of California—simply don't have significant legal protections with respect to the privacy of their digital data.

UP TO THE 1850S, MOST AMERICAN HOMES DIDN'T HAVE INTERNAL walls. Families lived, slept, washed, ate meals, and conducted every other activity in a single room;<sup>6</sup> even the livestock were housed indoors.<sup>7</sup> There were advantages to this arrangement: it meant only one room to heat, so everyone could keep warm from a single heat source. With animals to tend to and fields to plow, most of the family would spend the day outdoors anyway. Families generally huddled together just to eat and sleep—again, a warmer arrangement than being on one's own—so mornings and evenings were the only times when lack of privacy might have even been an issue.<sup>8</sup>

Physical privacy emerged as years went on for several reasons, health being key among them. With contagious diseases among the prime factors killing off 30 percent of all children in the year 1900, public health experts at the time urged parents to separate their children into their own beds if possible.<sup>9</sup> Beds, being expensive, then also became status

symbols: only the wealthy could afford to have separate beds for various individuals in their homes. However, privacy in the home is also a culturally specific phenomenon. In a study of 186 cultures, anthropologist John Whiting determined that 67 percent of all children were sleeping in beds with at least one other individual, child or adult, as recently as the 1950s.<sup>10</sup>

Physical privacy matters to this discussion because it's very difficult to have *informational* privacy without it. Imagine your spouse and siblings and children all sitting on the sofa with you. It'd be difficult to have a private phone conversation in that sort of setting.

While informational privacy is not a uniquely American phenomenon, it has its roots in the very founding of the country. The practice of being forced to house and feed British troops, codified in the Quartering Act of 1774, emerged as part of a series of measures instituted by the British following the Boston Tea Party as a means to get the colonists back in line. Better known by locals in America as “the Coercive Acts” or “the Intolerable Acts,” the colonists deeply resented these measures.<sup>11</sup> The very personal nature of housing troops from what was seen as an occupying force especially irked them, leading them to explicitly abolish the practice in the Third Amendment to the US Constitution—lesser in importance only than what's stipulated in the First and Second Amendments: the right to bear arms and freedom of speech. The Fourth Amendment also speaks to early America's concern with personal privacy: ensuring protection of one's property from illegal search and seizure.

Despite the interest in personal privacy in early America, until very recently the realities of life meant that privacy was still hard to come by, as noted above. Just as physical privacy was available only to the very wealthy in past centuries—those who could afford homes with walls separating all their rooms—informational privacy was available only to those who could afford to hire message carriers to deliver notes with relative certainty that their contents would remain at least somewhat secure.

It wasn't until well after the advent of modern technologies such as the telephone that Americans en masse could really experience privacy in the sense that we experience it today. Until the 1960s, most telephones were connected to what was called a "party line": a single number that you shared with your neighbors.<sup>12</sup> If you wanted to use the phone, you had to pick it up, determine if someone else was already using the line—maybe eavesdrop a little—then wait your turn. It wasn't until the popularization of the cell phone barely two decades ago that each individual could have a dedicated phone number that wasn't also shared with family members or coworkers. It wasn't a given, though: only 50 percent of Americans had cell phones as recently as 2002.<sup>13</sup>

One of the most startling observations about privacy in the information age comes from Vint Cerf. Cerf is widely considered one of "the fathers of the internet," having developed the file transfer protocol (the technique that lets you upload and download web pages, files, photos, and so on). He led DARPA (the Defense Advanced Research Projects Agency; the people who invented the early internet, called ARPANET) and founded ICANN (the Internet Corporation for Assigned Names and Numbers, the group that makes it possible for us to keep track of names like [www.google.com](http://www.google.com) instead of IP addresses like <http://74.125.224.72/>). He's now Google's chief internet evangelist—that's his actual job title!—working on the company's artificial intelligence team. In short, Cerf's no slouch. When he speaks, people tend to pay attention.

At an event at the Federal Trade Commission on November 19, 2013, Cerf, sporting his trademark three-piece suit—a habit that makes him one of the very few sartorially sophisticated tech gurus in the world—made a prediction that rattled the industry. "Privacy," he announced, "may be an anomaly."<sup>14</sup> Technology is what made privacy in the modern sense of the word possible in the first place, he argued, with "the industrial revolution and the growth of urban concentrations that led to a sense of anonymity." And privacy today is under threat, mostly because of our own actions. "The technology that we use today has far outraced our social intuition. . . . [There's a] need to develop social conventions

that are more respectful of people's privacy." But we're not anywhere close to that yet, he said. "This is something we're gonna have to live through."

Privacy matters, and not just as something we view as an inherent right. We behave differently when we know we're being watched than when we believe we're in private. It's called, fittingly, the "observer effect" or, for reasons explained below, the "Hawthorne effect."

Back in the 1920s, many Americans made their living in factories—34 percent of us, compared with just 5 percent today.<sup>15</sup> Taylorism, or the practice known as "scientific management"—designed to derive maximum efficiency from the workforce—had swept across industries. As part of this trend, from 1924 to 1932 a massive telephone equipment manufacturing facility in Illinois called Hawthorne Works underwent a series of studies, ostensibly to identify ways to increase labor productivity.<sup>16</sup> (The study was commissioned in order to "prove" that more lighting would lead to greater output, thus helping to sell more electricity.) Scientists noted that under certain conditions, worker productivity increased, while it decreased under other conditions—not solely to do with lighting, but also with other factors, including cleanliness of the workspace, timing of breaks, and so on. For decades, these studies influenced practices on factory floors, serving as a benchmark for the ideal quantity and quality of lighting, hygiene, and breaks necessary to eke out the utmost from factory laborers.

About twenty years later, a social scientist named Henry A. Landsberger took a closer look at the Hawthorne studies. He determined that it wasn't the lighting that had made the workers more productive. Rather, it was most likely the fact that workers were being paid attention to, even if only as subjects of a study.

Since Landsberger's observation, the Hawthorne effect has been widely studied, debated, debunked, revived, and otherwise dissected—mostly in an attempt to determine once and for all whether the Hawthorne effect was actually exhibited in the Hawthorne studies, as opposed to whether the effect actually exists at all.<sup>17</sup>

What the observer effect means is pretty intuitive: when we know we're being watched, we act differently than when we believe we're alone. In many cases, this means trying harder, also called the "social desirability bias": in short, people want to look good to others. So if we know other people are looking, we work a little harder to make ourselves appear appealing.

The question becomes, then, What happens when we feel as if there might *always* be someone watching? If all our digital activity is monitored, and—with an increasing deployment of public sensors and surveillance cameras in smart cities—our physical activity is monitored, does this mean we *always* try harder to look good? To contextualize why this matters, it's worth noting that the social desirability bias wields great power over us. It's so powerful that even depictions of eyes, as on a poster with people staring at you, are enough to make you modify your behavior for the better (called, appropriately, the "watching eye effect").<sup>18</sup> In one pilot test conducted in a police precinct in Nottinghamshire, England, hanging posters of watching eyes coupled with police warnings was credited with a 40 percent drop in theft.<sup>19</sup>

Although our behavior may improve due to the observer effect, we don't tend to enjoy the feeling of being studiously observed. Ever been in a crowded room and look up to catch someone who's clearly been watching you? People tend to describe the sensation as uncanny—creepy, even. And you're not psychic, by the way, when you catch an observer—you can thank your visual cortex, a part of your brain, for being able to notice someone's stare.<sup>20</sup> Here's how it works: In any given environment, there's too much stimulation to process all at once. Your eyes take in a vast amount of stimuli, but then your visual cortex helpfully divvies it up and sends it out to around 10 distinct areas of your brain. The region to which these information packets are sent depends on the nature of each stimulus: whether you perceive a threat, a familiar face, something confusing; they all get processed differently. In one study, a subject who was cortically blind—meaning, unable to consciously see anything—was given a series of faces to look at. Although he couldn't actually *see*

anything, the area in his brain that processes emotions around faces, the amygdala, still activated. This shows that our brains are working hard even when we don't know we're being observed, just in case it turns out that we *might* be observed.

Which all sounds really tiring. Think about it: Behave when you know when you're being watched. Straighten up when you know you're being watched. Be smarter, kinder, better, add-desirable-quality-here when you know you're being watched. We're so preoccupied with the possibility of being watched that our brain is alert for signs of observation even when we're not consciously aware of being watched. Add tech to the mix, and we create new opportunities to be watched. Whenever we post anything online—a photo on Instagram, a tweet, a Facebook post, an email—we're essentially throwing up a flag in the ether, saying, “Hey! Over here! Check me out!” And now we can add in the “internet of things”—sensors and surveillance cameras in everyday devices (such as refrigerators) that we don't traditionally think of as being online—as cities become “smarter” (more on that in chapter 6). Opportunities to be watched—both created by us and placed in our lived environment—multiply exponentially. If we actually made ourselves aware of all this watching, where would the cognitive drain leave us?

To better understand cognitive drain and why privacy is so important to us, we need to first understand what our brains are capable of. Scientists estimate our brain processing speed at approximately 120 bits per second.<sup>21</sup> As a frame of reference, to pay attention to one person talking eats up approximately 60 bits per second. To be in the presence of multiple people talking doesn't just *feel* overwhelming; it *is* cognitively, neurologically overwhelming. It exceeds the available bandwidth of our attention.

In this way, the trend toward net state investments in the physical world via the internet of things may be unwittingly helping us out. As it is, we don't pay much attention to net states. When we use our iPhone, we're likely not thinking of Apple, the company, or even of the phone as a device itself; we just *use* it. Similarly, we don't call to mind Google,

the company, when we send an email; we open up Gmail and just write the message. As net state products and services become more and more integrated into our lives, they become less noticeable. They become, as in Brooks's stem and flower metaphor, background; the infrastructure for our interactions: effective, familiar, and blissfully unremarkable.

This is important because demands on our attention have never been higher, and the trends suggest that these demands will only increase. Yet our attention has yet to evolve to the point where we can effectively process more stimuli, making us feel perpetually overwhelmed or exhausted or stressed out or some combination thereof.

Consider how we pay attention.<sup>22</sup> We do so in different ways depending on the circumstances: We pay attention to things around us—that's spatial attention. And we pay attention to things as they happen, which is temporal attention. Then within that temporal category are lots of subgroups. There's selective attention—as when you have to focus in on a friend talking to you amidst a crowded party; you have to tune out other conversations and pick out just what your friend is saying. There's sustained attention—as when you need total silence in order to focus on writing for long periods of time. Then there's alternating or divided attention—as when you cook; you have to go back and forth between checking a recipe and doing the chopping and measuring and what have you, alternating your attention between reading and doing.

The demands that today's technology places on our attention are largely temporal. If you look at your smartphone for a moment, you'll note that it takes up very little of the visual landscape. It's just not terribly taxing of spatial attention. Contrast this with, say, navigating a traffic jam on a busy city street. Strewn with billboards, storefronts, pedestrians, street lights, traffic lights, cars, trucks, motorcycles, cyclists—that's a packed tableau that'll suck spatial attention dry in a heartbeat.

Back to the phone: despite its relative smallness, it has an outsize ability to absorb us. Media stimuli—social media posts, games, news feeds, emails, texts—all soak up our temporal attention. And we can process only so much. In fact, if we get too many new bits of informa-

tion in rapid succession, our brains helpfully tune out some of them, in what's called the attentional blink.

The attentional blink is brief—about half a second—meaning that it's not going to help us tune out distracting notifications that pop up on our screen (usually twice, for upwards of 10 seconds). But knowing that our brains engage in attentional blink is an important reminder that we have limits. Our brains, which are astronomically more powerful than the world's fastest supercomputer, hiccup when they're overloaded.

This warrants a quick breakdown of the brain. That organ is more than a machine, of course, but if we were to simply regard the machine-like aspect of it—its processing power—we'd have to admit it's an absurdly powerful machine. In 2013, researchers set out to use the world's fastest computer—then Japan's Fujitsu-built K computer—to simulate human brain activity. They calculated that one second of brain activity involves 1.73 billion nerve cells firing on 10.4 trillion synapses.<sup>23</sup> Simulating one single second of human brain activity took this computer 40 minutes—a computer made up of 82,944 processors. (By comparison, the MacBook I'm writing on has one processor.<sup>24</sup> One.) The K computer used the equivalent of 250,000 PCs' worth of memory. To provide a point of comparison on memory, 250,000 PCs' worth is still small potatoes; scientists believe that the human brain holds about a petabyte of data, roughly the same amount of data floating around in the billion websites of the entirety of the internet.<sup>25</sup> This data is far more than details such as your kindergarten teacher's hair color or the formula for finding the area of a triangle. It encompasses such things as instructions that keep your nervous system functioning, your heart beating.

So that's your brain. Impressive, no? But even your brain—a machine so mighty that a supercomputer roughly 83,000 times more powerful than your laptop can simulate only a tiny fraction of its power—has a measurable limit to its ability to pay attention. And that limit is half a second. If you were driving 60 miles per hour, you'd cover a distance of 44 feet in half a second. That's about three midsize car lengths.<sup>26</sup>

Or, if you experienced an attentional blink, you might miss those

three car lengths. This precious resource, our attention, is somewhat fragile. When we've got our attentional wits about us, we can catch sudden changes on the road—a quickly braking car ahead of us, a deer, or a child chasing a ball. But despite how awesomely powerful it is, the brain rations attention, parceling it out to given stimuli depending on how important each one seems. And digital media—colorful, flashing, moving images especially—sure do seem important to the brain.

Net states recognize that we have only so much attention to give, so they take steps to help us help ourselves preserve it. Not for any altruistic reasons, though; if we burn out on digital media, they lose us as users. To combat attention fatigue, Apple recently rolled out Screen Time, an app that tracks how much time you spend per app per week and provides a weekly report that tallies it up for you.<sup>27</sup> Google plans a similar feature for its Android phones—this one will go so far as to gray out your screen when you've exceeded the limit you set for yourself.<sup>28</sup>

The digital realm needs to stay “healthy” in order to keep users there. It's in net states' best interests to invest in the health of that ecosystem—for example, by combating terrorists on their platforms (discussed in chapter 4). And an ecosystem is only as healthy as the creatures who inhabit it. We users of the internet need to remain attentionally healthy, so to speak, in order to be fit enough to stay online, let alone thrive online. And only if we thrive online do we generate data—the accumulation of which is the ultimate goal for net states.

“Privacy as we normally think of it doesn't matter,” said Aza Raskin, cofounder of the Center for Humane Technology—a technology watchdog group founded by Silicon Valley engineers—in a 2019 interview.<sup>29</sup> It's data the big tech companies are really after, he said. “Imagine it's a stick figure at first, and as you use the system, it's collecting fingernail scraps and bits of hair. What do you care that you lost a fingernail scrap? But they're putting it together into a model of you . . . little models, little avatars, little voodoo dolls of you.” The real problem with this lies not in your invasion of privacy, per se, but rather, in the fact that net states use your data to create models of you—not someone *like* you; *you*.

The questions become, then, What happens with these data models? And do we get any say over how they're used?

WHAT WE'VE LEARNED ABOUT THE COLLECTION OF OUR DATA THUS far has not made us happy.

Twenty years, a month, and a week after a then-youthful Bill Gates made his infamous appearance before Congress in the late '90s, on April 11, 2018, Facebook founder and CEO Mark Zuckerberg found himself in the very same hot seat. Facebook had been pilloried in the news for almost a solid year. First came the reports about the Russian misinformation warfare carried out on Facebook's platform during the 2016 presidential election. This was followed by the previously mentioned revelation that a political consulting firm, Cambridge Analytica, had gained access to 87 million users' private data without their explicit knowledge or consent.<sup>30</sup>

What was lost on the public is that this was in no way a data breach or hack or leak: Cambridge Analytica's access to user data is just one example of the kind of access scores of companies doing business with Facebook had, according to Facebook's 2015 business model (which they've since modified). Yet the public outrage either missed or ignored this fact. As technology writer Will Oremus pointed out, this may have been in part due to the fact that our collective rage at Facebook was not just because of what Facebook had done with our data; it was also because of our own gullibility for having given up so much of our information in the first place. "It was Facebook," he wrote, "that taught people around the world to freely give themselves online and to accept the use of their personal data in targeted advertisements as the price of admission to the modern internet."<sup>31</sup> And thus it was Facebook that received the brunt of the global ire. We had awakened to the fact that our data wasn't just being "liked" by friends and family members; our data served as the behind-the-scenes currency that businesses traded with Facebook in order to let Facebook proudly claim in public, "It's free and

always will be.”

Combined, the outcry over the two scandals torpedoed the public love affair with Facebook in a matter of months. Congress, which had largely ignored Silicon Valley in the two decades since the Microsoft hearings, finally had no choice but to confront its leadership head on. For the 2016 presidential election scandal, in November 2017 Congress settled with dragging just the lawyers from Google, Twitter, and Facebook before them in what ended up being a blustering nonevent with no consequences.<sup>32</sup> But by the spring of 2018, the public backlash following the Cambridge Analytica story had grown so intense, Congress had no choice but to pull in Zuckerberg himself.

Mark Zuckerberg had apparently taken note of Gates’s disastrous encounter with the Senate Judiciary Committee in 1998. In his own testimony, which spanned a total of 10 hours and addressed over 600 questions, Zuckerberg attempted to appear sober, respectful—chastened, even.<sup>33</sup> It didn’t always work. Over the two-day grilling by both the House of Representatives and the Senate, Zuckerberg sat on the receiving end of much finger-pointing and huffy indignation. But ultimately, the hearings revealed more about Congress’s lack of understanding about tech than anything Facebook had or hadn’t done with user data. In one epitomizing moment, 84-year-old Senator Orrin Hatch—the same senator who two decades earlier had effectively taken Gates to task—demanded of Zuckerberg: “So, how do you sustain a business model in which users don’t pay for your service?” With what has been characterized by numerous news outlets as a “smirk,” Zuckerberg replied, “Senator, we run ads.”<sup>34</sup>

While much news analysis has been written about the hearings themselves, they ultimately yielded no tangible legislative change nor any punishment for Facebook or any of the other net states that might be mishandling user data: Amazon, Apple, Google, Microsoft, and Tesla artfully blended into the proverbial wallpaper during the Facebook hearings and their aftermath.

The disappearing act worked for only so long, though. Google’s day

in court came next—not with the Patacsil case, which is still in preliminary stages, but with Congress. On December 11, 2018, Google CEO Sundar Pichai stood before Congress to defend the company's data-handling practices. But again, Congress missed its chance to reveal anything other than its own misunderstanding of the tech industry. In this hearing, it was Rep. Steve King (R-IA) who put his foot in his mouth, demanding to know why his granddaughter's iPhone displayed certain information. Pichai politely noted, "Congressman, the iPhone is made by a different company." King attempted to backpedal, but in that moment, the optics of who had power irreversibly shifted. What could have been a firm congressional investigation into the tech industry came off instead as a game of political point-scoring, patiently tolerated by the person who appeared to be the real grown-up in the room: Google's Pichai.

News reports following Google's hearing thus drew similar conclusions to those following Facebook's hearings: Congress had had yet another shot at bringing down our net state kings a peg, and they blew it.<sup>35</sup> As of this writing in 2019, despite increased public awareness in the United States about our lack of protections of our digital information, there remains no legislation to address it.

Legislation, though, may not be the perfect solution for protecting users' rights. "Tech will always change so fast that hard and fast legislation rules freeze you in the wrong place," Tom Wheeler, President Obama's chair of the Federal Trade Commission from 2013 to 2017, told me in an interview in January 2019. "What's ironic is that the very same tech companies that fought tooth and nail against federal regulations three years ago—here's a story for you; when they fought rules in Congress, they passed around a document detailing how, and I quote, 'privacy regulations would significantly *harm* consumers'—have now come around to *ask* for federal privacy rules."

When asked why he thought this was the case, Wheeler replied, "Now that they're seeing California with its own privacy regulations, they're seeing that other states will likely follow suit. There will be a plethora of rules. So now the tech companies themselves are advocating

for one set of federal rules that they can comply with, because if they have to deal with 50 sets of state rules, all of which are different, they won't be able to operate."

If the tech industry itself is advocating for federal regulations, why haven't they materialized? There are several superficial reasons. The first is a perennially gridlocked US Congress that has been so mired in partisan rancor for the past several years that it has been unable to pass sweeping legislation of any kind, let alone a package that might be considered controversial, such as a federal data protection law. Also, the US lacks a central agency that would oversee enactment of such laws even if they did exist.<sup>36</sup>

But the root cause of our lack of data protection laws in the US requires us to look inward, and it's a tad more depressing than partisan bickering: perhaps people just don't care enough about the issue to push for change.

In what *Atlantic* writer Ian Bogost has termed "privacy nihilism," one of the reasons people fail to take the requisite steps to safeguard their digital data is simply preemptive exhaustion, a communal malaise. We sense that our data's already gone; that we lost the privacy battle before we even knew it was ours to fight. As such, there's no point in getting all up in arms about it now.<sup>37</sup> In a 2017 Pew Research Center study on trust in online platforms, experts identified this trend, noting that whether we trust our tech (or not) may not translate into action regarding our *use* of that tech. Trust, or the absence of it, will simply become "irrelevant," they predicted. "Hacking, identity theft, trolling, doxxing"—when someone reveals another person's personally identifiable information publicly online—"will become increasingly commonplace and a daily cost of doing business on the internet."<sup>38</sup>

Research supports that this trend will likely continue. According to a 2018 study by the University of Michigan, people who purchase "smart" home devices like Google Home or Amazon Echo (detailed more in chapter 6) are fully aware that they're risking their private information being collected; they've simply given up on the idea of privacy.<sup>39</sup>

“What was really concerning to me,” said Florian Schaub, assistant professor at the University of Michigan and one of the study’s coauthors, “was this idea that ‘it’s just a little bit more info you give Google or Amazon, and they already know a lot about you, so how is that bad?’”<sup>40</sup> She concluded, “It’s representative of this constant erosion of what privacy means and what our privacy expectations are.”

We’ve become so inured to news stories about data breaches, data leaks, and untrustworthy personal privacy policies that we don’t even bother to read them anymore (if we ever did). Which is ironic. More and more privacy notices are being written in plain English as tech companies attempt to comply with the European Union’s recent data regulations. So it’s now more *possible* to read them than ever. The question is, Will it make any difference if we do?

For instance, if you live in Vermont and you’re having a Powerwall installed in your home, as described in chapter 2, you may have the opportunity to read and sign Tesla’s privacy notice—which is totally doable; it’s not even two pages long and is written in accessible English. But what about Tesla’s Powerwall partnerships directly with cities such as Norwich, Connecticut, and San Jose and Santa Ana, California? Will their residents be notified that Tesla may collect their personal information? Will they even know that Tesla is a partner in running their electrical grid?

Here’s why this matters. A sentence in the “How We May Use and Share Your Personal Information” section of Tesla’s privacy notice reads: “We may share Personal Information we collect with *third parties* when necessary to perform services on our, or on your, behalf” (italics added).

Who are these “third parties”? The notice doesn’t say. But if Tesla is anything like the majority of businesses that collect consumer data in the United States, “third parties” most likely include data brokers.

Data brokers are essentially what they sound like they would be: companies that buy and sell your data—for gobs of money. They’re a \$50-billion-a-year industry in the United States. Yet despite their massive financial assets, they operate largely in the dark; most Americans

have never heard of even the biggest among them, which include Acxiom, Nielsen, Experian, Equifax, and CoreLogic.<sup>41</sup> “Most [people] have no idea who these companies are and how they got their data on them,” commented Amul Kalia, who works for the Electronic Frontier Foundation, a consumer privacy advocacy organization. “And they would be very surprised to know the intimate details that these companies have collected on people.”<sup>42</sup>

While Tesla and Google and Facebook gather personal and behavioral information on their singular platforms, data brokers—so powerful that one reporter referred to them as “the whales of the data ecosystem”—compile it all to create comprehensive and detailed profiles.<sup>43</sup> A 2014 report by the Federal Trade Commission showed that one data broker, Acxiom, had databases storing 3,000 “data segments” on just about every individual consumer in the United States.<sup>44</sup> In some cases, these segments reflect our religious preferences, with labels like “Bible Lifestyle”; our economic circumstances, like those of us who fit into the categories “Financially Challenged” or “Modest Wages”; our marital status, like “Working-Class Mom”; and our entertainment preferences, like “Media Channel Usage—Daytime TV,” “Exercise—Sporty Living,” and “Outdoor/Hunting & Shooting.”

This data segmentation doesn’t stop at the behavior associated with the products we buy. We’re also sorted into categories based on our overall lifestyle, such as “Rural Everlasting”—that would be single men and women over the age of 66 with “low educational attainment and low net worth”—or “Downtown Dwellers,” those of us who are “upper-middle-aged” and with a “high-school” or “vocational/technical” degree working to “make ends meet with low-wage clerical or service jobs.”

While this may feel too high on the creepy spectrum, the data brokers themselves attempt to paint such specific market segmentation as actually good for us. For instance, on Acxiom’s website section “How Personalized Marketing Works,” they display two kinds of ads: what you’d see if you were a, say, 46-year-old single male—that would be an ad for a flashy red sports car; and what you’d see without personalized

marketing: an ad for—heaven forbid—makeup. Another example: if you’ve recently moved, Acxiom shows that you’d see ads sharing the opportunity for 20 percent off “housewarming” furniture; without personalized marketing, they display some dreary impersonal credit card pitch that clearly doesn’t know how to congratulate you properly on your big move.

With these examples of the ways that “personalized marketing” is “helpful,” we can begin to see how our personal data gets monetized. Because if I’m in the business of selling flashy red sports cars, I probably really do want to target single men in the midlife crisis range. Plain old common sense suggests that they’re a more likely buyer group than, for instance, women with young children. With the amount of money American businesses spend on advertising—\$218 billion in 2018—it’s not hard to imagine that they’d want to ensure that those dollars are spent targeting the absolutely most likely buyers, down to zip code, lifestyle, age, parental status, and other relevant variables.<sup>45</sup>

The question then becomes, How can data brokers compile enough information to know not only our demographic details, but how far we went in school, the kind of job we have, how much we earn, and whether we have kids, hunt, or go to Bible study?

That would be from the “data elements” they collect from various companies. They may learn about our vacation habits from the companies we buy our plane tickets from, like Expedia<sup>46</sup> or Kayak.<sup>47</sup> Our weight, height, educational attainment, and parental status may come from dating sites like Match.com<sup>48</sup> or OkCupid.<sup>49</sup> One dating site, Grindr, even shares users’ HIV status with data brokers—if the users voluntarily shared this information with the site, it’s unclear whether this in violation of HIPAA protections.<sup>50</sup> Our political affiliation, credit card use, occupation, net worth, and other data elements are regularly collected from just about every company and online service we do business with.

The true value for data brokers isn’t individual data elements or even the marketing segments they sort us into. Instead, the value resides in the aggregation of data that allows them to create a finely detailed pic-

ture of who you are—again, not someone *like* you; specifically *you*—and what you’re likely to need. “The extent of consumer profiling today means that data brokers often know as much—or even more—about us than our family and friends,” said Edith Ramirez, then chair of the FTC, in a May 2014 press release.<sup>51</sup>

What’s even more alarming about our data profiles is that they’re not limited to information available digitally. Thanks to a process called “onboarding,” data brokers collect information about our offline habits to include in our profiles as well: things like magazine subscriptions, what we purchase with store loyalty cards, and publicly available data from government records.<sup>52</sup> “The marriage of online and offline is the ad targeting of the last 10 years on steroids,” said Scott Howe, chief executive of Acxiom, in 2014.<sup>53</sup> Onboarding is how it’s possible for you to stop at Target to buy DayQuil and then, when you log on to your computer a few hours later, see ads popping up on Facebook for humidifiers and throat lozenges.

What’s the big deal? you ask. What possible data could a company like Tesla sell to a data broker about your energy use that would matter to you? Think about it: When do you turn the lights on? When you wake up. When do you turn them off? When you leave your house. On again? When you get home from work. Off again? When you go to sleep. And so, using just your energy use data, Tesla and whoever they sell your data to have your daily routine mapped out to the minute. They know, in general, when you will be home. More important, they know when your home will be empty—and potentially vulnerable to any criminal who might want access to it.

This is a problem because all digital data—*all* of it—is hackable. And hacks have happened. Equifax, one of the three largest credit score firms in the United States as well as a major data aggregator and broker, suffered a massive cybersecurity breach in 2017 that left 143 million Americans’ data exposed.<sup>54</sup> Whoever stole this information could theoretically use your data profile to find out where you live and—if they have access to your energy use profile—when you’ll be out during the

day.

Consider the Equifax breach and Tesla Powerwall side by side. Much of your personal information is floating around in the ether, thanks to the Equifax hack (and perhaps other hacks that we're not yet aware of; Equifax waited two months before reporting the breach).<sup>55</sup> This data profile includes who you are, where you live, what you like, where you work and shop, what you earn, and—thanks to Powerwall—when you're home and when you're out.

Assume also you're one of the 47.5 million Americans—that's one out of every five of us—who also has access to a voice-enabled assistant such as Amazon Echo, Google Home, or even your iPhone's Siri.<sup>56</sup> Smart speakers are also hackable, and hacks are well documented. For instance, researchers at the vulnerability testing firm Checkmarx demonstrated that it was “surprisingly easy” to gain remote access to an Echo and have it record everything it hears—all without notifying the user.<sup>57</sup>

Hacks, however, are the worst-case scenario. The more likely outcome is that net states willingly give—“share” is the more popular term—your data to third parties. Amazon, for instance, is currently considering giving third-party developers access to the transcripts of user conversations recorded via the Echo. Google Home already does.<sup>58</sup> This means that in addition to the content of your conversations—what you say you want, where you're going, what you're arguing with your spouse about—they have a new piece of biometric data: your voice. The iPhone X already has a fair bit of personal biometric data, including your thumbprint (if you enabled that login option) and your facial features (if you enabled Face ID). With voice-enabled assistance, it adds your voice to the data pool as well. Data brokers already have behavioral profiles on the majority of Americans; with the next generation of technology, they'll be able to add physically identifying characteristics to the profiles as well.

It may be that Google and Amazon and other purveyors of voice-enabled assistants collect user conversations simply to improve their products. Yet regardless of how innocent their rationale may be, the

question remains: What happens to our data once we share it? Even though the original data collector may have our permission to possess our information—which we gave when we signed their terms of service—if the language contains any reference to third-party sharing, we may as well kiss our privacy goodbye.

OUR RIGHTS AS CITIZENS ARE PROTECTED THROUGH THE BILL OF Rights in the US Constitution. Most of us are generally familiar with the big ones that pertain to us: freedom of speech, assembly, religion, and so on. But how our rights extend to the data *about* us is unclear. For instance, the Fourth Amendment says that we are protected from unlawful search and seizure. This means that no one can take our property—that we should “be secure in [our] persons, houses, papers, and effects,” to be precise—without a legal warrant.<sup>59</sup>

Is our personal data our property? What exactly *is* personal data? These types of thorny questions are currently being hashed out in the halls of the European Parliament. The world’s strongest data protection legislation to date came out of the European Union (EU)—the 2016 General Data Protection Regulation, better known as the GDPR, which took effect in May 2018.

The GDPR introduced a new term for the residents whom the legislation protects, calling them “data subjects.”<sup>60</sup> By contrast, the tech companies that collect information about data subjects are “data controllers.” Under the GDPR, data subjects—Europeans from 28 countries—are granted a slew of rights, including the right to consent to how their data is collected, the right to be notified within 72 hours of a data breach, the right to know what their data is being used for, and, perhaps most important, what’s known as the “right to be forgotten”—or “data erasure,” to use the technical term. Should a data subject withdraw consent at any time, the data collector must stop using his or her data or face heavy fines: 4 percent of the company’s annual global turnover, or 20 million (roughly the same as \$20 million).

That a bill of rights for data subjects exists somewhere in the world is a huge step in the right direction for users. Citizens of the EU now have explicit rights with respect to their personal data. Put another way, Europeans have rights on multiple levels. They have rights as citizens of their individual nation-states *and* as members of the EU, the latter role now conferring rights as “data subjects.”

This is a totally laudable move; it’s great that such legislation exists somewhere in the world. But it’s problematic in practice.

As with all diplomatic endeavors, there’s the issue of enforcement. At present, each individual member state of the EU—again, 28 different countries—will have its own enforcement mechanism. That’s 28 different methods for making sure every tech company that interacts with its citizens complies with GDPR requirements.

To consider what this means in practice, think about our phones. The average user accesses 30 apps on their smartphone each month and has about 90 apps total installed.<sup>61</sup> About 502 million people live in the 28 nations that compose the EU. This means—even if we’re just talking about the 30 most commonly used apps a month—that the supervisory authorities are responsible for ensuring that tech companies comply with the GDPR in 15,060,000,000 (more than 15 *billion*) citizen-user tech interactions a month. It would be the understatement of the year to note that oversight authorities in the EU are going to have their hands full.

And it’s just not clear how oversight is going to work. At present, the GDPR stipulates that there be “one GDPR supervisor per country.” According to Article 54, it’s up to each of the 28 member states to determine how to set up its Data Protection Authority (DPA) and Supervisory Authority: how many people should staff their offices, how they should operate, and what level of funding they’re allotted by their own government.<sup>62</sup>

Put another way, GDPR supervisors in Belgium, Slovakia, France, Germany, and Estonia may all operate completely differently from one another, function with different budgets, and be given varying levels of priority within their home country, depending on their local political

climate. So, while there's an oversight board for all DPAs—that would be the European Data Protection Board—as with all things GDPR, “many details still needed to be hammered out” (the official GDPR characterization of the situation).<sup>63</sup>

Enforcement issues aside, the GDPR is all well and good for the Europeans. But what does it mean for us Yanks? For the tech industry as a whole, it means a lot of compliance catch-up. In the days preceding the May 25, 2018, deadline, you may have noted a flurry of email notices in your inbox about privacy policies for various tech services you've registered with (and some, perhaps, that you didn't even know you were registered with). Despite having more than a year's notice that the GDPR was coming, a lot of tech companies simply didn't make the deadline. For instance, when the GDPR took effect, several major American news sites, including the *Los Angeles Times*, the *New York Daily News*, the *Orlando Sentinel*, the *Chicago Tribune*, and several others simply went offline to anyone in Europe.<sup>64</sup> Deciding that GDPR compliance simply isn't worth the hassle, a number of tech companies—for example, the massive multiplayer online game Ragnarok, the advertising services Verve and Drawbridge, the Brent Ozar Unlimited consulting company, the Unroll.me email manager, and the security company Steel Root—have ceased doing business with EU users.<sup>65</sup>

Meanwhile, a month before the GDPR took effect, Facebook moved 1.5 billion users—more than half its global user base—out of reach of European regulators and to its HQ in California.<sup>66</sup> As privacy researcher Lukasz Olejnik noted, this was a massive undertaking: “Moving around one and a half billion users into other jurisdictions is not a simple copy-and-paste exercise,” he said. The end result? “Users will clearly lose some existing rights, as US standards are lower than those in Europe,” he noted. Given the scale of the user base moved, as well as the timing, it's difficult to imagine that Facebook had anything else in mind with the move. Facebook and other net states can do what they like with user data in the United States. So long as we keep using their products and services, many of them will continue to persist as they have.

In the United States, regulations focus on the *product*—the information itself and how it’s handled—not on the user having any inherent rights. Take, for instance, HIPAA, the Health Insurance Portability and Accountability Act of 1996. HIPAA protects a person’s medical information from being shared without consent. If you’ve been to a doctor’s office in the past 20-plus years, you’ve probably signed a HIPAA consent form (probably without reading it) that gave permission to release or share your medical information. Note, however, that HIPAA doesn’t give *you* any special rights. Rather, it carves out special protection for one subset of data *about* you—your medical information—and what a certain group of people—medical professionals—can do with it.

Another example is what’s known as PII: personally identifiable information. This includes the combination of name, date of birth, Social Security number, and other data that, in aggregate, would give away key details about a person’s legal identity. PII is protected under the Privacy Act of 1974, which establishes a “code of fair information practices,” basically spelling out what federal agencies can and cannot do with the records they keep on citizens.<sup>67</sup> As with HIPAA, though, this regulation focuses on what certain groups of people—in this case, federal officials—can *do* with a certain type of information.<sup>68</sup> Once again, a certain type of information *about* us is regulated, but we as citizens aren’t afforded any special protection.

Compared with residents of the European Union, American citizens don’t have data protection rights. We are not “data subjects” here. We are citizens of our nation-state with respect to our physical selves and our physical environments. And we are users of our net states with respect to our digital selves and our digital environments. At present, net states have free rein, as stated earlier, in terms of what they wish to do with our personal data (with the exception of medical information). But they’re not all reacting to that freedom in the same way.

Some net states are taking a more user-centric approach of their own volition. Microsoft, for instance, is actively expanding “data subject” rights: they’ve launched a “privacy dashboard” that permits any tech

user in the world to sign up for GDPR-level privacy protections.<sup>69</sup> And some Americans are taking advantage of that feature.

As Microsoft president Brad Smith noted during our interview in September 2018, “When we made those data subject rights available to customers on a global basis, in the European Union itself, a market with over 500 million people, there are roughly a million plus people who took advantage of that. In the United States, a market of 320 million, there were two million people who took advantage of it.” He said, “It really, I think, should cause people to reflect on what is a longstanding view that people often present the United States, including in the tech sector, that Americans don’t care about these issues the way Europeans do. Well, there’s something there that Americans got pretty interested in.”

AS DISCUSSED ABOVE, NET STATES ARE ESSENTIALLY GIVEN FREE REIN in the US but are subject to new, strict regulations in Europe. But Europe’s not the only place that net states are facing backlash from nation-state governments. In May 2018, Uganda, in an attempt to wipe out “gossiping,” enacted a tax on social media use:<sup>70</sup> 200 shillings a day, or \$0.0531—about \$19 a year. It may not sound like much, but in a country with an annual GDP of \$615 per capita, it’s not nothing. In Papua New Guinea, a small island nation in the South Pacific, authorities banned Facebook for a full month.<sup>71</sup> “The time will allow information to be collected to identify users that hide behind fake accounts,” commented Communications Minister Sam Basil. Facebook and other social networking sites such as Instagram and WhatsApp have also been the target of scrutiny by governments elsewhere, such as Cambodia, Myanmar, Sri Lanka, and the Philippines.<sup>72</sup> While there are very likely less than noble reasons for enacting these bans—clamping down on free speech from citizens, journalists, and advocates high among them—the upshot is that not every nation-state is giving Facebook or other tech platforms free rein in their sovereign territories.

In short, in 2018, 33 nation-states—the 28 EU members plus the aforementioned—suddenly became much more difficult places for net states to do business. Given this, it's probably not surprising that net states are looking to set up shop *outside* nation-state borders. All the land on Earth is currently governed by nation-states, but two categories of Earth's territory have yet to be clearly claimed and regulated: outer space and the deep sea.

In 2009, Google was awarded a patent for seafaring data barges: offshore data centers that could traverse international waters.<sup>73</sup> While Google has yet to build any such barges, other net states are beginning to explore what the seas have to offer them.

The ocean offers distinct advantages. Data centers—the machine hubs where our online information is processed, transported, and stored—are physical computers housed in physical structures that consume tons of energy. According to the United States Data Center Energy Usage Report, data centers in the territorial US are projected to consume approximately 73 billion kilowatt-hours by 2020.<sup>74</sup> To translate that into English, charging your smartphone for a full year requires 1 kilowatt-hour. To keep the internet going, however, requires 70 *billion* kilowatt-hours—or, as one reporter described it, “equivalent to [the output of] about 8 big nuclear reactors.”<sup>75</sup>

For this very reason, chilly Scandinavia has become a popular destination for net state data centers: companies have opened centers in Denmark (Apple), Iceland (Facebook), Sweden (Amazon), Norway (Microsoft), and Finland (Google).<sup>76</sup>

In 2015, Microsoft launched Project Natick, a pilot program to sink self-contained data centers in the ocean. The idea was first floated in 2013 in a white paper—one of the coauthors had worked on a Navy submarine—and by 2015, Microsoft decided it was worth throwing some money at it.

“When I first heard about this I thought, ‘Water . . . electricity, why would you do that?’” said Ben Cutler, one of the engineers for Project Natick, in an interview. “But as you think more about it, it actually

makes a lot of sense.”<sup>77</sup> Computers crash when they overheat. That’s expensive. Cooling them with air-conditioning demands lots of electricity. That’s also expensive. Storing all this machinery requires valuable physical real estate. *That’s* expensive. The ocean undercuts costs in all three areas. The currents keep the machines cool while also powering turbines. Theoretically, these turbines could convert the ocean currents into electricity, and there you have it: functional, powered data centers that are cool enough to keep from melting down.

There are also potential legal advantages to investing in sea-based data centers. There’s certainly plenty of physical real estate: more than 70 percent of the planet is covered in ocean.<sup>78</sup> The United Nations Convention on the Law of the Sea (UNCLOS) established that country borders extend exactly 12 miles offshore. Considering that there are about 332,003,271 cubic miles of ocean, clearly the majority of that undersea sector doesn’t fall under the purview and protection of any nation-state.

By now Project Natick is more than just an idea. In June 2018, Microsoft dropped a pilot data center off the coast of Scotland in collaboration with the European Marine Energy Center.<sup>79</sup>

“We see this as an opportunity to field long-lived, resilient data centers that operate ‘lights out’—nobody on site—with very high reliability for the entire life of the deployment, possibly as long as 10 years,” said a Microsoft spokesperson. The company also projects that it can manufacture underwater data capsules in as little as 90 days, significantly faster than it takes to construct traditional land-based centers.

The possibilities here are more than a little intriguing. Data centers can be created and deployed in just a few months. And there’s no reason they can’t be dropped, say, 13 miles off the coast—just a smidge outside the bounds of nation-state sovereignty. In theory, the data centers would not be subject to the nearest nation-state laws or regulations. Rather, they would fall under the UNCLOS, which, while well intentioned, is effectively toothless in terms of enforcement. In short, net states could operate their data centers, which could theoretically house all our personal data, beyond the reach of any nation-state. If they did,

net states—not nation-states—would have sovereign domain over their citizen-users. The sea would set them free.

## FOUR



# INFORMATION-AGE WARFIGHTERS

As much as we experience life online, we are creatures of the physical world, vulnerable to physical threats. This chapter explores our physical security, showing how net states like Google can aid in the fight against modern-day enemies. Analyzing the differences between the tech ethos and the military ethos, this chapter explores how the expertise so prized by security agencies has become a potential disadvantage in the fight against terrorism. It shows the possibilities for net state/nation-state cooperation through acts of diplomacy and notes how net states, led by Microsoft, have begun to forge ahead in this domain.

“We Love Death More Than You Love Life,” reads the bold-print Facebook post in the video. The shot cuts back to a young man seated in what looks to be a dining room, his face masked by a blue-and-black checkered keffiyeh pulled up so high it almost obscures his eyes.<sup>1</sup> The video names him “Abo Abdullah.” He stares at his interviewer just off camera. “A year ago,” he says before taking a long pause, “I joined ISIS.”

The YouTube video, entitled “Captured ISIS Fighter on How He Was Betrayed,” is slick, professionally produced—the product of an American digital news outlet called Vocativ, founded in 2013. “What did

your leaders tell you about America?” the interviewer asks off camera. Abdullah hunches forward, lifting his right hand to cradle his head. “They used to teach us that Americans were atheists who deserved to be slaughtered.” He rubs his forehead; stops talking.

The video, which runs about five minutes, details how Abdullah was recruited into ISIS from his home country of Saudi Arabia, arriving in Syria under cover of night. He tells how he believed that he would become a martyr “for the crimes committed against Islam”; how he went through a closed-camp, 30-day training program in which he wasn’t permitted to communicate with anyone on the outside; how, once in the camp, “they start to indoctrinate you, . . . ‘Don’t trust this,’ ‘Don’t trust that.’”

In the video, Abdullah wipes sweat from his brow with his sleeve when he gets to the part about how he ended up leaving ISIS. “I was captured,” he says, “during a battle between ISIS and FSA [the Free Syrian Army, opponents of Syrian president Bashar al-Assad].” He says, “The FSA told me, ‘You can be sold for cash—why did you come here to fight?’ That’s when I realized I had been sent to my death by ISIS.”

This video is one of dozens of ISIS defector videos that Google and a counterextremism organization, Moonshot CVE, leveraged in a pilot test to deter ISIS recruits.<sup>2</sup> For eight weeks in 2018, rather than finding ISIS-related propaganda, users who typed “How to join ISIS” into Google’s search engine were redirected to 116 different counternarrative videos detailing the dark side of ISIS—ISIS defector videos like the one described above, for instance, or homemade videos showing ISIS fighters languishing in long food lines, undermining the narrative that the caliphate was a well-provisioned paradise.<sup>3</sup> During the pilot, in addition to serving up anti-ISIS videos, Google featured ads for mental health services alongside user’s search results.<sup>4</sup>

The campaign worked surprisingly well: it reached 320,906 users during the test period. Users who had started out searching for terrorist recruiting materials instead ended up watching 500,070 minutes of video of counternarratives.<sup>5</sup> The mental health content worked even bet-

ter: users who entered the most violent search terms ended up clicking ads for psychiatric support at rates 115 percent higher than a control group.<sup>6</sup> The campaign diverted more than a thousand potential terrorists from recruitment materials and sent many vulnerable people to resources for psychological help.

This isn't an unusual approach for a counterterrorism campaign. What makes it unusual is who was running it: not the US Department of Defense or the CIA or any other national security agency. It was Google. And they weren't doing it for profit. Google made a moral judgment here. Indeed, by placing their own ads on the site (in lieu of selling space), they lost out on potential revenue that they could have earned. They also acted against their primary business practice: to facilitate search for their users. In this case, Google worked with the express purpose of luring users *away* from the content they were searching for.

It's worth noting that Google wasn't simply the business broker in this equation. The company was acting as a quasi-counterterrorism agent, having made a policy decision to intervene in normal business processes to achieve a greater good. Antonia Raithatha, senior digital communications of Moonshot CVE, the counterextremism organization Google partnered with on this, emphasized in an interview that it was Google's understanding of users, not just Google's tech, that made the campaign successful. These campaigns need to tap into "non-ideological drivers of extremism that recruiters use to sway vulnerable individuals," she explained. You have to understand users' desire for "the sense of purpose and belonging." This desire—to be a part of something bigger than oneself, to have a clearly defined purpose handed to you—that's what recruiters tap into to lure prospects.

In this respect, Google had an advantage over, say, the Department of Defense. Google's counterterrorism strategy was based not on policy directive, but rather on a deep understanding of what their users want; something at which a search engine—pry to our most private questions—is uniquely expert.

This particular campaign was a success, though most of us have

probably never heard about it. This raises some questions: When *else* does Google intervene in searches? Do they redirect people seeking information about nefarious conduct across the board? Or only in cases of terrorist activity? And who at Google makes that decision? Does the company have some sort of counterterrorism wing, or was this just an experiment cooked up by some do-gooder engineers?

One answer, it turns out, is that Google does indeed have a department devoted to counterterrorism and other campaigns for the public good. It's called Jigsaw.

CHELSEA MARKET IS, ON THE FACE OF IT, AN UPSCALE FOOD HALL. Situated just beneath Manhattan's elegant elevated park, the High Line, its ground floor offers a variety of shops ranging from "The Heatonist"—specializing in artisanal hot sauces—to the quirky "Artists & Fleas." The 51 rather pricey shops nestled in its charming, brick-walled halls attract well-heeled tourists and tote-bag-wielding locals alike, giving it a bustling, almost European feel.

What most people don't know is that in February of 2018, Chelsea Market was purchased by Google.<sup>7</sup> And just inside its 10th Avenue entrance, tucked away behind what appears to be an exotic pillow and lamp shop, stands a glass door with stairs leading up a flight to Google's geopolitical think tank, Jigsaw. Formerly known as Google Ideas, Jigsaw was founded in 2010 by then CEO Eric Schmidt. Its mission: to use technology to "tackle the toughest geopolitical challenges, from countering violent extremism to thwarting online censorship to mitigating the threats associated with digital attacks."<sup>8</sup>

I met Jigsaw's managing director, Scott Carpenter, in his office on a Tuesday morning in July 2018. Once inside Jigsaw's suite, you'd never know that a sea of shoppers meandered the floor below. In keeping with standard tech company architecture, an open pit hosted rows of tables that served as desks for multiple people, each work space piled with dual monitors, quirky decorations, and what looked to be at least two

cups of coffee per staffer. Carpenter ushered me into his office, one of Jigsaw's few closed-door spaces, which he shared with another senior leader.

I dove in with the basics: What's Jigsaw up to? And what's in it for Google to "tackle the toughest geopolitical challenges"?

"If the internet is our ecosystem in which we live, breathe, and operate and make all of our money," Carpenter replied, practiced and patient, "we need to think about what are the ways in which we need to protect that ecosystem."

A former senior State Department official, Carpenter is mild-mannered and deceptively low-key—an intellectual powerhouse in the guise of a smiley-eyed tech evangelist. He and I were halfway through what felt like an easy conversation when I realized he had been unwinding carefully selected anecdotes to contextualize a grand global narrative. Like great politicians, Carpenter has a way of making you feel totally at ease—charmed, even—while wowing you in a humble, understated way. Like the best of nations, Google chooses its leaders wisely.

"In the same way, you protect the Gulf of Mexico if you're BP," he mused. "Understanding that [terrorists] are a threat to your existence if you don't, [we asked ourselves,] What can we do?"

The tricky part is figuring out the how: How precisely do you go about protecting an ecosystem of over 1.5 billion websites?<sup>9</sup> According to Carpenter, Google is open to discussing the question of how with absolutely anyone. Information-sharing is, after all, core to the hacker ethos. "I led a group to northern Iraq to talk to former ISIS fighters in detention facilities," he reflected. "But we'll talk to the CIA, too."

However, "talk to" is where Google draws a self-imposed line. "We'll talk to anyone," he said. "But we're not going to *collaborate* with governments."

The CIA is certainly part of the American government, I almost pointed out. But then I reminded myself that "talk to" may mean sharing information, exchanging ideas even. But that's just conversation—a far cry from engaging in some sort of active collaboration.

“Any governments?” I asked.

“Yeah,” he nodded, cool but firm. “And that’s kind of a principle.”

Whether we like it or not, net states don’t need governments nearly as much as governments need net states. One example where this is painfully evident is with attacks on official computer systems.

“We are dealing with a hostage situation,” Atlanta mayor Keisha Lance Bottoms noted almost casually at the hastily assembled press conference. Standing flanked by a troupe of commissioners and city council members on March 22, 2018, her team took turns detailing the enormity of the problem their city now faced.<sup>10</sup>

After approximately ten minutes of damage reports, the mayor herself returned to the microphone. “It’s an attack on government,” she noted, poised, unruffled, “and, therefore, an attack on all of us.”

The hostages in this case weren’t people; they were computers used by the 424 programs—around 30 percent of which were deemed “mission critical”—that served as the foundation for Atlanta’s government. Due to a ransomware attack, the 8,000 employees using the city’s computer network were locked out, their machines either compromised or completely disabled.<sup>11</sup> An entire city government—one that served over 5.7 million residents—had been effectively shut down.

Scrambling for solutions, the city of Atlanta did what most local government officials would do—they called in the feds. The FBI and the Department of Homeland Security were immediately engaged to investigate the source behind the attack.

But not even the FBI would be able to bring Atlanta’s systems back online; FBI agents are investigators, not computer experts. So Atlanta made another call—to the tech industry itself. Microsoft, Dell, and several other tech firms launched into action to free the hostages data and render the systems operational again.

The ransom was, relatively speaking, a paltry sum: \$51,000. By contrast, the tech contracts cost the government of Atlanta \$2.7 million.<sup>12</sup> But as the FBI noted, there was no way of knowing whether the ransomers would cease the attack if they got their money. Also, Microsoft was

a trusted entity. If government was going to pay, clearly they felt it was safer to spend millions of dollars on Microsoft, a trusted ally, than any amount on unknown criminals.

And the tech firms did indeed deliver. They restored access to the computer network in just six days, recovering the vast majority of the compromised data. As Atlanta recovered from its attack in the months to follow, the overwhelming advice they heard was this: “Back up your files to the cloud”—specifically, to net states cloud services: Google Drive, Apple’s iCloud, Microsoft Azure, or Amazon Web Services.<sup>13</sup> Notably, the advice was *not* to create a government version of the cloud; rather, government officials and tech experts alike advised the same approach—to use the cloud that exists, despite the fact that it had been created and was managed and safeguarded not by government but by net states.

As the Atlanta case shows, net states are both governments’ digital suppliers and cyber defenders. They create the platforms governments run on, the storage citizen data resides in, and the search-and-rescue forces called upon when public data falls under attack. In the digital age, government—whose essential job is to protect citizens—is finding that it can’t always protect even itself. That government is calling on net states like Microsoft to bail them out and Google or Amazon or Apple to back them up reveals a shift in power that is the hallmark of the rise of net states.

Another example can be seen in the case of the Russian misinformation campaigns that infiltrated social media during the 2016 presidential election. These practices were not, in fact, a new phenomenon. According to a comprehensive study of Russian misinformation commissioned by the Senate Intelligence Committee, the attacks started about five years prior. Since then, “disinformation has evolved from a nuisance into a high-stakes information war.”<sup>14</sup>

Congress finally took some steps to understand the phenomenon, in the form of commissioning the above-mentioned report (in 2018, two years after the election). But despite multiple US official confirmations

that Russia was behind these actions, the federal government has failed to offer any tangible help to the tech companies on whose platforms this warfare is being waged. Net states are essentially on their own to deal with the information wars waged using their services.

To win these information-age wars, countries need to recognize the power of net states as not just allies, but coequals. Net states wield the kind of power and influence necessary to go toe to toe on digital warfare with other nation-states, like Russia, as well as nonstate actors, like ISIS. As recently as 2017, the American government didn't seem to be getting this.

"I don't think there's ever been a technological advance that governments have been able to keep up with," reflected Carpenter during our 2018 Manhattan interview. "I think governments still don't understand enough about what they're doing—the brain surgery they're doing without understanding anything about the brain."

As I first described in the 2017 *WIRED* article that inspired this book, the world needs net states because they occupy the digital space where warfare is manifesting, with tactics like disinformation warfare by other nation-states as well as recruitment and organizing attacks by nonstate actors.<sup>15</sup> As such, net states like Google understand the norms and tactics of digital warfare—the brain surgery Carpenter referred to—far better than a Cold War-era strategist ever could. Major General Michael K. Nagata, former commander of the American Special Operations forces in the Middle East, circled around this idea back in 2014. In a leaked confidential conversation about ISIS, he said, "We do not understand the movement, and until we do, we are not going to defeat it. We have not defeated the idea. We do not even understand the idea."<sup>16</sup>

The notion that ideas are a national security consideration is not a new one: since 9/11, the United States military has been trying to win "hearts and minds" of combatants in Iraq and Afghanistan.<sup>17</sup> Despite this, the military establishment has been slow to recognize the potential of net states to assist in the fight against radicalization. It appears that military leaders have instead continued to view net states simply as

keepers of the platforms where recruiting and organizing occur, rather than as real assets in the fight, savvy insiders with unique insights into how terrorists move and operate.

Our enemies learned long ago how to exploit the digital landscape for their purposes. Terrorists have proven themselves to be extremely adept at using net state platforms—social networking tools like Twitter and Facebook; encryption tools like Snapchat, WhatsApp, and Telegram; and video-sharing platforms like YouTube—to organize attacks, recruit members, and spread disinformation.<sup>18</sup> In one study, researchers who looked at terrorist activities across 96 countries found that recruiters routinely found new would-be terrorists through Facebook’s “Suggested Friends” feature.<sup>19</sup> And Facebook itself admitted that terrorists and other criminals likely used its encrypted messaging platform WhatsApp as a secure communications tool.<sup>20</sup>

But knowing how misinformation spreads or how terrorists recruit online isn’t enough. National security agencies and the military need to put themselves into the mindset of tech-savvy digital warfighters. But they can’t do this without first becoming tech-savvy themselves. Here I’m not talking about knowing how to *use* technology; I’m talking about having a handle on the tech *ethos*, grasping it deeply and intuitively.

For such a tech-heavy institution, the military just doesn’t seem to “get” tech. This is not to say that they don’t *understand* technology. Far from it. They are steeped in extremely advanced technology in most aspects of their work. But *using* tech is different from having a tech *ethos*. And the military ethos and the tech ethos couldn’t be more different.

In many ways, the tech ethos is an outgrowth of the hacker ethos: but instead of describing how to *make* tech, it describes how to *use* tech. The best expression of the tech ethos I’ve ever come across is from internet pioneer and MIT professor David Clark. He said, “We reject kings, presidents and voting. We believe in rough consensus and running code.”<sup>21</sup> Putting primacy on openness and information-sharing rather than on blind allegiance to formal authority allows everyone to have a say, which is why the best ideas, more often than not, rise to the top. In

other words, tech embraces what *works*, as opposed to what's procedurally *approved* to work. Like the hacker culture described in chapter 1, the tech ethos holds that skill matters, not credentials. Authority comes not from what fancy college you went to or title you might hold, but from who can make tech work better, period. According to the tech ethos, a 17-year-old hacker living in his mom's basement or a cybersecurity expert at the Pentagon are equals, if they can code equally effectively.

One of the reasons that the military fails to "understand the idea" (to echo Nagata's wording) behind the tech ethos rests with its reliance on experts. National security circles are filled with experts: policy experts, cybersecurity experts, military strategists, grand strategy experts. Of course, experts are indispensable: we absolutely need to draw on the deep wisdom and practical know-how of people who understand every nook and cranny of their field.

The problem with experts in national security, however, is the governmental practice of relying *only* on experts. In Philip Tetlock's 2006 book, *Expert Political Judgment: How Good Is It? How Can We Know?*, he showed, after decades of data collection, that experts run into two problems when it comes to making predictions about upcoming threats.<sup>22</sup> First, expertise can lead to overconfidence. Since experts can rely on a deep well of existing knowledge, they might overlook the importance of gathering information in real time or double-checking their assumptions. Second, while experts tend to specialize in one thing, our increasingly complex world is also in need of generalists with multidisciplinary knowledge—knowledge that helps them connect seemingly unrelated things. Tetlock likens these two groups—experts and generalists—to hedgehogs and foxes, modeling his analogy on the philosopher Isaiah Berlin's essay "The Hedgehog and the Fox." Berlin adopted the phrase from the Greek poet Archilochus. "A fox knows many things," Archilochus wrote, "but the hedgehog one important thing."

In a 2007 lecture, Tetlock argued that foxes are, in fact, better at predicting what's going to happen in the future precisely *because* of their lack of expertise.<sup>23</sup> Generalists make predictions by considering a wide

array of real-time information, double-checking their assumptions, and reading up on areas they may not be familiar with. Generalists don't have a deep knowledge base to rely on. As a consequence, they're more willing to relinquish ideological loyalty and adjust their hypothesis when they uncover new facts. On the other hand, "partisans across the opinion spectrum," he noted, "are vulnerable to occasional bouts of ideologically-induced insanity."

Expertise is associated with confidence. "Blinded by beautiful theory," as Tetlock describes it, experts have a tendency to overly rely on their knowledge base and are, in general, less willing to adjust their predictions based on changing circumstances or new information. The political forecaster, as Tetlock puts it, who "bores you with a cloud of 'howevers' is probably right about what's going to happen. The charismatic expert who exudes confidence and has a great story to tell is probably wrong."

The Ivy-trained Tetlock didn't rely on his own expertise to come up with this theory: he tested it.<sup>24</sup> First, he studied those in the know, examining the aggregate predictions of 284 experts making 28,000 forecasts.<sup>25</sup> Then he studied nonexperts, launching a decade-long social science experiment called the "Good Judgment Project."<sup>26</sup> Sponsored by the Intelligence Advanced Research Projects Activity (IARPA, the US government's think tank for intelligence project moonshots), Tetlock invited volunteers to participate in online political forecasting exercises, in which teams of strangers tried to predict the outcome of a political election or a world event. (The project is ongoing—you can sign up to be a forecaster yourself on [www.gjopen.com](http://www.gjopen.com).)

Among the 2,000 participants in the initial group, Tetlock identified a small group of "superforecasters," foxlike generalists who out-forecasted the experts.<sup>27</sup> In a tournament that pitted five research teams of generalists against professional intelligence analysts with access to classified data, Tetlock's superforecasters outperformed the intelligence analysts in accuracy at every turn.<sup>28</sup> According to Steven Rieber, program manager at IARPA, "Team Good Judgment . . . beat the control

group by more than 50%.” What’s more, he noted, “This is the largest improvement in judgmental forecasting accuracy observed in the literature.”

Despite evidence like that generated from the Good Judgment Project, unfortunately generalists don’t make it very high up the promotion ladder in national security agencies. This is because such agencies hire and promote based on credentialed expertise. And therein lies the problem.

Again, there’s a good reason to value expertise in the intelligence community. In a refreshingly sober assessment of what it takes to work in the intelligence field, “So You Want to Be an Intelligence Analyst,” former analyst Matthew Burton writes, “The primary point of intelligence analysis is not to defeat current threats. Instead, it is to foresee, prepare for, and prevent tomorrow’s threats. . . . When the next unforeseen threat arrives, it’s very important that the policymakers have immediate access to expertise—expertise attained through years of quiet research.”<sup>29</sup> A slew of experts in the intelligence community churn out reports on Ukrainian ethnography, to use Burton’s example, *just in case* this topic later proves to be valuable in assessing an emerging threat.

However, as Tetlock’s investigations show, we *also* absolutely need generalists: foxlike adaptable thinkers who can scan the horizon and make assessments based on the facts of the day, not a lifetime of research. The tech ethos, which prizes in-the-moment capabilities over long-earned credentials, is thus grossly mismatched with the military ethos, which prizes earned credentials above all else.

While achievements during time in service matter, the primacy placed by the military on needing to simply do time in your job is out of joint with not only the tech ethos, but also with the threats the military faces today, which are unpredictable and increasingly tech-based. Combined, the military’s time in service requirements and the up-or-out promotion schedule—if you don’t get promoted on schedule, you’re out of a job—skew the national security workforce toward people who have been in their field forever. As veteran military journalist Leo Shane

put it, these policies prevent bringing in people qualified “to tackle specific challenges—issues like cybersecurity—because [those] individuals don’t have the requisite time in service to step into senior leadership roles.”<sup>30</sup>

ONE MILITARY EXPERIMENT, HOWEVER, TRIED TO INCORPORATE THE tech ethos into a military operation. In 2004, General Stanley McChrystal, then commander of the Joint Special Operations Command (JSOC), was eager to change the United States’ strategy in Afghanistan and Iraq. Desperate to turn around two poorly faring wars, the career military man uncharacteristically adopted critical elements of the tech ethos into his battle plans. As McChrystal describes in his book *Team of Teams: New Rules of Engagement for a Complex World*, the military in 2004 wasn’t set up to win—in the most literal way possible.<sup>31</sup> Its bureaucratic chain of command and siloed sources of information were simply too cumbersome to compete with the networked command structure of al-Qaeda. McChrystal recognized that there was one exception: small teams within the armed forces—such as the Special Operations forces—also managed to be agile, fluid, and networked. But he couldn’t figure out, in the parlance of Silicon Valley, how to scale the qualities that made Special Ops so effective to the entire armed forces.

“It was impossible to foresee what elements of our organization would and would not need to know a given piece of information,” McChrystal noted. “So instead of trying in vain to control information, we reversed direction and shared it as broadly as possible. . . . Our motto became ‘share until it hurts, then share some more.’”<sup>32</sup>

While keeping intact the command structure that has dominated the US fighting forces for centuries, McChrystal instituted three key changes to operationalize this radical form of information-sharing. First, he modified that hierarchical command structure to include “boundary spanners,” or people who could “provide critical links between two groups of people that are defined by functional affiliation, physical lo-

cation, or hierarchical level.”<sup>33</sup> Just because the military relied on hierarchy, McChrystal realized, didn’t mean that everyone on the same tier was equally qualified for every task. Some people are more social than others; some are connected to lots of people above and below their official rank. These are the “boundary spanners”—the “culture carriers,” as McChrystal’s former aide-de-camp Chris Fussell termed them in his book *One Mission*. This is similar to Malcolm Gladwell’s conceptualization of the people he calls “connectors” in *The Tipping Point*.<sup>34</sup>

Whatever we call them—boundary spanners, culture carriers, or connectors—we intuitively “get” who these people are: people who just seem to know everyone else. McChrystal recognized the value of people who could span boundaries and quickly granted them permission to consult with members of the military above and below their rank. This empowered the boundary spanners to share information throughout the chain of command via informal networks, not unlike how gossip spreads through neighborhoods.<sup>35</sup>

McChrystal then instituted a daily 90-minute video conference call, the “Operations & Intelligence Forum,” or O&I, which allowed thousands of soldiers of different ranks around the globe to participate in the briefing. The purpose of the call was, on one level, to go over the previous day’s events, establish what was on the docket for the hours ahead, and ensure that everyone understood their respective assignments. But, as Fussell describes it, the O&I was more forum than traditional meeting. McChrystal encouraged participation, setting an example in how he presented his own reports: “McChrystal had to lead from the front,” Fussell explained. “First, he himself had to share all news, whether positive or negative. Second, he had to show during the meetings that he was nonjudgmental about the news, whether positive or negative.”<sup>36</sup> Doing so set the tone that enabled others to come forth with their potentially less than stellar news or partially fleshed-out ideas.

The O&I simultaneously served two critical purposes: (1) to enable boundary spanners to emerge on any level of any team; and (2) to let McChrystal reiterate daily what he called the “aligning narrative,” a re-

minder that everyone on the call, regardless of rank, was part of one mission, something bigger than any of them as individuals.

McChrystal's O&I shows that even the military, the country's most rigid hierarchy, can bring elements of the tech ethos into their operations. True, the O&I forum was not exactly an example of "rough consensus and running code," as Clark had described the tech ethos, nor was it an example of rejecting "kings, presidents, and voting." But it was a hybrid model that embraced the emphasis of the tech ethos on collaboration, inclusion, and openness to ideas, all within the firm scaffolding of the military hierarchy that would run the call, deliver the narrative, and, once the call was concluded, issue orders throughout the remainder of the day.

The need for our security forces to "get" the tech ethos grows by the day. While physical threats to our collective security remain, more and more threat actors lob their opening salvos digitally.

On October 25, 2018, approximately 50,000 military and civilian support personnel from 31 NATO member states and partner countries assembled in Brydalen, Norway, a tiny town known primarily for a church constructed in 1884 by the entirety of the town: twenty residents. Brydalen was one of several sites on land and just off the Norwegian shoreline hosting "Trident Juncture," the largest NATO military exercise in northern Europe since the end of the Cold War.

"It is happening in the air, on land, at sea and in cyberspace," NATO's website explained. Quoting Admiral James G. Foggo, commander of Allied Joint Force Command Naples, the site read, "Trident Juncture will show the world that NATO is relevant, unified, and ready to defend itself in this Article 5 scenario, testing our collective defense."<sup>37</sup> With temperatures dipping down to the low 20s overnight, the operation was clearly intended to test not only coordination of land, sea, and cyberspace response, but the physical rigors of cold weather warfare. It is likely no coincidence that the region selected for Trident Juncture was at roughly the same latitudinal coordinates as those between St. Petersburg and Moscow, Russia.

With NATO's shift from Afghanistan and the Middle East to activity in Europe and North America, cold weather warfare is coming into focus as a necessary skill to develop. "NATO has standing forces in Poland and the Baltics, and these are also very cold areas. The Alliance needs winter knowledge," notes Major Knut Hummelvoll, chief for the Norwegian School of Winter Warfare.<sup>38</sup> "Cold knowledge," he reports, is a growing interest among militaries, especially in the United States and the UK. In 2017, the school held 1 course for 30 participants. In 2018, they saw a 1,900 percent increase in enrollment, forcing them to expand from 1 to 10 courses, now accommodating 60 participants apiece.

Despite careful planning and precision execution, just a few days after Trident Juncture launched, officials detected a serious problem: NATO's GPS system had been jammed.<sup>39</sup> Scrambled GPS signals threw off communications among the 50,000 participants and threatened aerial maneuvers for the military aircraft as well as commercial airlines, which transported upwards of a million passengers for the duration of the exercise—from October 25 to November 7.<sup>40</sup>

Norwegian and Finnish defense agencies traced the jamming to Kola Peninsula, site of a heavily fortified Russian base just over 200 miles southeast of the Norway-Russia border. The US denied that the GPS jamming was a problem, telling CNN it had "little to no effect on US military assets" during the NATO exercise. NATO spokesperson Oana Lungescu was slightly more transparent, telling reporters, "Jamming of this sort is dangerous, disruptive, and irresponsible."<sup>41</sup>

This wasn't the first time the Russians had been caught deploying GPS-jamming technologies against the US military. In April 2018, NBC News reported that four American officials had confirmed Russia had been jamming US military drones operating in the airspace over Syria, causing them to malfunction or crash.<sup>42</sup> Todd Humphreys, the director of the Radionavigation Laboratory at the University of Texas at Austin, said the impact of these tactics was significant. "They are a little less hostile looking than a kinetic bullet," he said, "but sometimes the effect can be just as damaging. It's like shooting at them with radio waves

instead of bullets.”

Here’s where net states could be helpful partners to the military: working in concert to develop effective anti-GPS-jamming systems. But net states have yet to step up to the table. Despite all the monetary incentives for nabbing a military contract, most net states simply don’t seem to be interested, as Google’s Project Maven (described in the introduction) exemplified. The question remains, then, How can the military change tech companies’ minds?

THE US GOVERNMENT / NET STATE HEAD-BUTTING DESCRIBED IN THE introduction—both Microsoft’s battle with the Department of Justice and Google’s retreat from the Pentagon—may be celebrated by net state employees who lean more toward the hacker ethos than the military one. But where does this leave the nation-state, which is responsible for pursuing justice for and physical protection of its citizens? The military’s frustration at being left behind by net states was eloquently expressed by First Lieutenant Walker D. Mills, a US Marine Corps infantry officer, who wrote an open letter to Google: “Dear Google, please help your country defend itself.”<sup>43</sup>

In the letter, Mills argued that while Google’s staffers may feel morally superior by cutting ties with the defense industry, they’re not necessarily making the country—or even themselves—safer. “Neutrality, even well-intentioned, is not possible,” wrote Mills. “We live in a world where Facebook’s platform has been corrupted to influence our elections and terrorists use the secure messaging of WhatsApp and Telegram to coordinate their crimes.” He added, “In the pleading words of Merry from the ‘Lord of the Rings’ trilogy: ‘You’re part of this world, aren’t you?’”

Mills’s letter embodies a barely contained freak-out within the American military establishment—why can’t we get American tech firms to work with us?—on a very human level. The American defense community has been scrambling to convince tech companies such as

Google and Apple to work with them for years now. Having discovered that net states aren't offering themselves up as willing partners, the military has begun reaching out to cash-starved startups directly, with the promise of fast-tracking prototypes with plenty of funding.

For instance, in 2018, the Army opened its newest unit, the Army Futures Command—part of the Army's first major reorganization effort since 1973—in the notoriously liberal city of Austin, Texas, which has a burgeoning startup scene.<sup>44</sup> One of the first actions the Army Futures Command pursued was to set up two cross-functional teams, one of which is the Assured Position, Navigation and Timing Cross-Functional Team (APNTCFT)—or, in lay terms, the deal-with-the-GPS-problem team.<sup>45</sup> William Nelson, director of the APNTCFT, said they're working simultaneously on two tracks: first, developing methods to deploy pseudolite (from “pseudosatellite”) transmitters—sort of like ground-based, hyperlocal satellites—that can deliver a high-powered signal that's difficult to interfere with; and second, pursuing “software solutions to prevent jamming.” GPS and the technologies that are reliant on it—drones, for example—are priority one for the Futures Command: the very first event they hosted in Austin was called “Hack of the Drones.”<sup>46</sup>

The other military branches are also trying to address GPS and drone vulnerabilities. In 2016, the US Naval Academy reintroduced courses on celestial navigation—how to plot a course by the stars—which it had discontinued over a decade ago.<sup>47</sup> And not to be outdone by its counterparts in the Army, in March 2019 the US Air Force announced it would hold its own “Pitch Day,” a New York City-based event designed to attract startups and investors. As an Air Force official told me in an email describing the event, “It's a high priority for the Secretary of the USAF [United States Air Force] and she wants it to be known the USAF is ‘open for business.’”

Despite these outreach efforts to the cash-hungry startup community, the defense sector is finding a chillier welcome than hoped for. Their messaging probably hasn't helped. For instance, the Army Futures Command mission statement leads with the goal of being better able to

kill people. It states, “The Army’s modernization strategy has one focus: make soldiers and units more lethal.” Given Google’s mutiny over the very hint that its AI technology might be used to harm humans, the Army’s choice to lead with lethality language underscores just how much the military fails to understand its tech audience.

To be fair, it’s no mystery that this is what the military is designed to do: war isn’t like boxing in a ring, with rules and penalties. *It is* about killing people. But if the goal was to engage the tech sector in modernization of the military, plenty of other approaches for partnership would have been more effective. For instance, there’s a long history of military-technological innovation they could have pointed to: past partnerships led to the creation of the internet itself (first as ARPANET), GPS, encrypted communication, and scores of other hugely useful inventions.

The military’s choice to woo tech companies with words of aggression rather than of collaborative innovation reveals its failure to understand that the tech ethos isn’t just a mindset; it serves as a sort of moral compass for many in the tech industry. Sometimes, money alone isn’t enough. Certainly, the moral aspect doesn’t deter every net state from working with security forces altogether. Amazon, for instance, holds the contract for the CIA’s cloud services. Microsoft provides the cloud services for the Immigration and Customs Enforcement agency. But the idea that a code of ethics influences the broader industry at all—and that it’s ubiquitous enough that the military, the best-funded military in the world, is caught flat-footed in their quest to get the tech industry to work with them—reveals that many tech devotees want to do more than just code. They want to *build*: to contribute to some idealized, upgraded version of the world they’re in. And formal authority—whether it be the military, the president, or the king—is less important in this quest than whether those who create tech generally believe in the worth of what they’re creating.

In addition to highlighting past partnerships in innovation, there is yet another route the military could take to working with net states on securing the nation-state. This is to pursue partnerships on the flip side

of defense: diplomacy. That would be a wise place to start, especially given that net states are already making historic moves diplomatically that would have been unthinkable just a decade ago. Let's start with the "Digital Geneva Convention."

When Microsoft's Brad Smith announced that the cyberfield was a battlefield back in March of 2017, he also argued for the world's first diplomatic treaty on behalf of the tech industry—one that would help regulate internet-based conduct. The Cybersecurity Tech Accord, often referred to as the Digital Geneva Convention, was officially announced just a year later, on April 17, 2018. Thirty-four of the biggest global tech firms, including Microsoft, Facebook, Cisco, Dell, Oracle, and LinkedIn, pledged their support, though Google didn't join until the following year (and Apple and Amazon have yet to join at all). Within the next six months, they brought an additional 37 tech companies on board, internationalizing the group with the addition of the Japanese manufacturers Hitachi, Nokia, and Panasonic.

I met Brad Smith for an interview at Microsoft's Washington, DC, outpost not many months after the Tech Accord was signed. It happened to be the day after President Donald Trump's infamous speech at the 2018 United Nations General Assembly. As a reminder, in response to Trump's boasting of his administration's accomplishments, the audience erupted into an unprecedented outburst of laughter. Unfazed, Trump continued. "We reject the ideology of globalism," he told the more than 140 presidents, prime ministers, and kings gathered before him. "We embrace the doctrine of patriotism."<sup>48</sup>

The nation-state—America, specifically, ostensibly the most powerful nation on earth—is backing away from multilateralism. By contrast, the tech industry—Microsoft, Facebook, and the other signatories to the Cybersecurity Tech Accord—are embracing it, binding themselves together under a set of principles aimed not at protecting their business, but rather, at the global good: the rights of citizens.

Despite having just flown in from an Orlando, Florida, event with the comedian Trevor Noah, when we met at 2:30 p.m. on a Wednes-

day afternoon in September, Smith appeared remarkably alert, his eyes beaming with curiosity. With a congenial air that made me feel like we were just two buddies having a chat, Smith walked me through why Microsoft had taken the step to create the digital equivalent of the Geneva Conventions: “It’s definitely our view that a world with rules is better than a world without them,” he said. “It doesn’t mean that there won’t be people who violate them, but at least you have rules to point to when the violations take place.”

That a collection of the world’s most influential tech companies likened the Tech Accord to the Geneva Conventions—a series of diplomatic treaties signed by all 193 countries in the United Nations, pledging to protect civilians during times of war—signifies that this was a big deal. But one particular piece is the real reason this treaty is of moon-landing significance: principle 2, point 2, which states, “We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.”<sup>49</sup>

Again: the keepers of the digital world told the governments of the physical world, including their *own* governments, that they will not use their platforms, software, or any other tool or service for the purpose of waging cyberattacks. They declared themselves neutral—a “digital Switzerland,” as Smith termed it in his 2017 speech.<sup>50</sup>

Significantly, the signatories of the Tech Accord are not distinguishing among *citizens* of any particular *country* in their declaration of protection. Instead, they’re pledging to protect any and all tech users—the people who employ their products and services—*regardless of the nation-state in which users physically reside*. In establishing this accord, net states cemented the notion that a new class of citizen had sprung into existence: the previously discussed citizen-user. Though the accord didn’t use this specific term, it implied that individuals have rights that exist independent of whatever other rights they may have by virtue of the particular nation in which they live. Perhaps most significantly, in signing this treaty, Microsoft and Facebook and their allies have acknowledged their own power as players alongside countries. As the pro-

viders of both the battlefield and the weapons for the next generation of warfare—cyberwar—they have declared that they play a role in influencing diplomacy.

Smith reflected on the irony of this during our meeting. “When we sit down with the other companies that are headquartered in other countries [outside the US], we find ourselves perhaps more the spear-carriers for multilateralism at the moment than governments themselves.” He paused. “I don’t know that it’s healthy. We’d much rather be in a different place, but it is where we are.”

Smith explained how Microsoft and Facebook and their tech partners hoped to expand the Tech Accord’s impact later that year. “We’ve been working with a number of different stakeholders and our hope is . . . that governments can sign as well. . . . How governments, in particular, step up to embrace those [principles of the accord] could be very important.”

By any measure, they succeeded. In November 2018, the principles underlying the Digital Geneva Convention were folded into an international initiative sponsored by French president Emmanuel Macron. Called the Paris Call for Trust and Security in Cyberspace, this was the first-ever diplomatic accord between nation-states, net states, private-sector businesses, and not-for-profits. Fifty-seven countries, 70 tech firms, 188 private-sector businesses, and 112 not-for-profit organizations signed the Paris Call. This historic diplomatic agreement not only metaphorically but literally signified a new kind of power-sharing among different groups of global players, with company names affixed beside those of countries, on the same level, as coequals.

DIPLOMACY IS MORE THAN MULTILATERAL TREATIES AT INTERNATIONAL conferences. The day-to-day work of diplomacy resides in issuing official statements.

That may sound like a snoozer of a topic: “issuing official statements.” But it represents a seismic shift in how companies (and similar

entities) communicate to government, about government, and with government.

Take, for example, the matter of augmented reality (AR). It's pretty new tech. As such, it makes sense that it's yet to be regulated. But precisely because it's so new, we can use AR as a test case for why regulation is crucial. With AR technology, as with all digital technologies, the big question comes down to what happens with the data the devices collect. If net states already know us through our digital lives—Amazon, through what we browse and buy; Google, through what we look up; Facebook, by whom we connect with—then AR-powered net states will add to our profiles those currently missing elements about our *physical* lives: where we go, what we see, and which people we interact with. To ensure that we don't end up in some dystopian future where personally tailored advertisements pop up in our AR-mediated physical environment (as in the film *Minority Report*), we need to ensure that we're paying attention to how AR develops and, what's more, how it's regulated.

US regulation of net state technologies has been largely absent up to now, as we saw in the previous chapter. All we really see is a growing list of official statements. Amazingly enough, it's not government issuing those statements; it's the net states.

In July 2018, Microsoft released a statement calling on lawmakers to regulate facial recognition technologies. Now, the fact that Microsoft, whose cloud platform, Azure, is used by the Immigration and Customs Enforcement agency (ICE), came out against the practice of using facial recognition tech *may* have been a PR move. While it may have been fueled by genuine moral outrage, perhaps it was an attempt to defuse any implication of Microsoft's involvement with ICE, which in 2018 was wildly unpopular due to the brief but terrible practice of separately detaining immigrant parents and their children. Whatever the motive, the issuing of statements on this topic by net states was widely adopted: other tech companies that might have been considered remotely associated with ICE's family separations—including Apple, Google, and Facebook—issued statements of condemnation as well.

The significance of net states issuing statements of condemnation against a government can hardly be overstated. Statements of condemnation are generally issued *by* governments criticizing activities by *other* governments. For instance, the US State Department issued 93 statements of condemnation from 2017 to 2018 alone, on topics ranging from hostilities in South Sudan, Russia's violations of Georgian sovereignty, the criminalization of protests in Venezuela, and attacks on security forces in Egypt.<sup>51</sup> Official statements are *governments'* way of talking to each other. They're bureaucratic turf. To see tech companies embracing official statements of condemnation sure makes it seem like they're adopting governmental practices.

Here's why statements matter in diplomacy: they are the first move one country takes against another in a chain of potentially escalating events. By themselves, they may seem toothless to the casual observer: How far does saying "This is bad" or "We call on So-and-So to change" actually go toward fixing a bad situation? one might wonder. But issuing an official statement is like moving the first pawn in a game of chess; it declares intent against the other party, who, through this act, becomes the opponent. That statement may stand alone, the game never further engaged in. On the other hand, it may turn out to be the *first* step, the next move being official talks. Official talks may then be the precursor to official actions. This is where things go up a level. Because official actions invariably hurt: they include economic sanctions, military strikes, war.

For tech companies to issue official statements—in this case, to condemn the United States government—was almost unheard of a few years ago. Indeed, Microsoft had issued only three statements against government entities prior to calling on lawmakers to regulate facial recognition technologies: one condemning family separations in 2018, one on the CLOUD Act governing overseas data access, also in 2018, and one in response to the European Union's statement of objections in 2009. But the fact that it and other net states are starting to take up the practice is a sign that it's something we should be paying attention to.

Take, for example, the Trump administration's first travel ban, which barred visitors from seven Muslim-majority countries from entering the United States. Apple, Google, Facebook, Intel, and Expedia (owned by Microsoft) all came out with public statements against the policy.<sup>52</sup> Apple's Tim Cook, Amazon's Jeff Bezos, Google's Sundar Pichai, and others also signed a group letter calling on Congress to institute protections for so-called DREAMers—immigrants born abroad but brought to the United States as children.<sup>53</sup> "As entrepreneurs and business leaders, we are concerned about new developments in immigration policy that threaten the future of young undocumented immigrants brought to America as children," read the joint statement. "We call on Congress to pass the bipartisan DREAM Act or legislation that provides these young people raised in our country the permanent solution they deserve."

Now, again, these official statements of condemnation could cynically be construed as PR moves: both the travel ban and the family separations were hugely unpopular, making the companies that condemned them look good in the eyes of the public. But the more significant issue is the very use of the official statement of condemnation against a government—not by another government, but by an industry. That practice further underscores the quasi-state status that net states are growing into and is likely a sign of more activity in this area in the future.

AT THE HEIGHT OF ITS REIGN, ISIS CONTROLLED SO MUCH PHYSICAL territory in Syria and Iraq that it rivaled Great Britain in size.<sup>54</sup> ISIS wielded power over a population of approximately 8 million people, and through the banks, oil fields, mines, and other resources on its land it raked in \$2 billion in 2014 alone. It was, as one reporter put it, "the most powerful, wealthiest, best-equipped jihadi force ever seen."<sup>55</sup>

Three years later, ISIS's physical footprint was gone. Its nominal capital in Raqqa, Syria, fell in October 2017. From its peak fighting force of 20,000 to 30,000 in 2014, ISIS recruits have largely scattered to the wind, their primary connection with one another being on digital platforms.<sup>56</sup>

ISIS first gained power through those same digital platforms. Just because their physical presence has been defeated doesn't mean we should believe that terrorism itself has been defeated. ISIS's attraction to recruits was never solely about land. ISIS, and other terrorist groups, fed on recruits' fear, targeting the vulnerable, the disaffected, the marginalized; encouraging them to take action on their own—regardless of whether they were on ISIS-controlled land.

And they did. From when ISIS declared its caliphate in June 2014 through February 2018, ISIS or ISIS-inspired terrorists carried out 143 attacks in 29 countries, killing 2,043 people<sup>57</sup>—and 14 of these attacks occurred *after* ISIS had been officially defeated. Indeed, ISIS hasn't disappeared; they've simply relocated. Since the caliphate's fall in October 2017, the US Department of State has identified four new ISIS-linked terrorist organizations: ISIS-Bangladesh, ISIS-Philippines, ISIS-West Africa, and ISIS-Greater Sahara.<sup>58</sup> And ISIS continues to find connections and recruits via net state tools and services—most notably, Twitter and Facebook.

But perhaps what's more concerning for the average American isn't the threat of terrorists who are officially defined as such, but rather the so-called lone wolf attackers. There's no one profile that fits all lone wolf attackers, but they do tend to be motivated by personal grievances rather than political goals.<sup>59</sup> And they're on the rise, especially in the US: in the six-month period between January and July 2018, there were 205 mass shootings in the United States that together killed 214 people and injured 832, all perpetrated by lone shooters.<sup>60</sup>

Research suggests that social media may be contributing to the rise in mass shootings. According to a study conducted by Harvard University researchers, the rate of mass shootings in the US has tripled since 2011.<sup>61</sup> While no single reason was identified in that study, other researchers have noted what's called the "contagion effect": an average of 13 days following a mass shooting, a subsequent mass shooting is more likely to occur—indeed, between 20 and 30 percent of mass shootings appear to stem from the contagion effect.<sup>62</sup> Wall-to-wall media exposure

inspires would-be copycats. Studies further suggest that social media exacerbate this effect: in 2000, pre-social media, there were about three mass shootings per year. By 2015, this had escalated to 29 per year, or an average of one mass shooting every 12.5 days.<sup>63</sup> And it's only gotten worse since then: according to statistics from the Gun Violence Archive, between January and July 2018 an average of one mass shooting occurred every single day.<sup>64</sup>

As social media gained widespread popularity—2011 being widely regarded as the tipping point for that—would-be mass shooters both heard more about other shootings and were more able to envision their own rising fame should they take similar action, thanks to social media. While various motivations drive mass shootings, Jennifer B. Johnston, a researcher at Western New Mexico University, noted, “Unfortunately, we find that a cross-cutting trait among many profiles of mass shooters is desire for fame.” The quest for fame, she said, is “in correspondence to the emergence of widespread 24-hour news coverage on cable news programs, and the rise of the internet during the same period.”<sup>65</sup>

Social media outlets don't just spread the idea of mass shootings; many shooters post about their intentions *on* social media before acting. Following the Parkland, Florida, shooting in 2018, 600 copycats posted similar threats across social media targeting other schools.<sup>66</sup> The problem is, law enforcement doesn't have the capacity to investigate every single threat they encounter. According to one report, the FBI received 50,000 tips in the month of January alone.<sup>67</sup> Even if, as the report suggested, they get only about 100 “actionable” tips per day, that's still a staggering amount of potential evidence to wade through.

This is where “defeating the idea”—again, Nagata's words—becomes so important. Chasing threat-makers is a Whac-a-Mole exercise, making it virtually impossible to fully explore every potential threat.

Here's where net states could help: they have more than just data; they have user profiles. With these profiles, law enforcement could potentially narrow down who among the threat-makers is likely to take action.

This is not to suggest that net states hand over user data to law enforcement. Rather, net states have the opportunity to put their user data to use for public safety and security—an opportunity that they don't seem to be taking advantage of at this point. While Facebook has a significant counterterrorism (CT) team—with 200 staffers at last count—it is unclear whether these same individuals also seek out what could be called domestic terrorists: mass shooters. What is even less clear is what Facebook's CT team would do with the information if they *did* find potential bad actors. It's unclear what kind of relationship, if any, they have with the FBI, the Department of Defense, or local law enforcement. As citizens whose tax dollars fund law enforcement and national security agencies, and as citizen-users whose activities online make it possible for platforms like Google and Facebook to exist, we should expect transparency about the relationships between our net states and our nation-states.

Living as we do in the physical world, we must seek transparency from any and all entities that could do more to help ensure our physical safety from violence: whether that violence be from foreign or domestic terrorists, mass shooters, lone wolves, or however else malevolent individuals might be described. Net states might not be able to “defeat the idea” that inspires bad actors alone. But they are certainly better equipped to identify both the ideas that inspire and the actors inspired by those ideas than are governments working on their own on the outside.

Keeping a country safe from violent offenders in the information age means understanding that the goalposts are constantly moving and adapting in real time as the actors and targets change. Governments need net states; and net states—as keepers of the ecosystem in which terrorism plots are hatched, planned, and reported on—need to consider sharing their insights with governments. They should do so safely, securely, to be sure—but in some kind of partnership. The health of the internet ecosystem and all its inhabitants would be better for it.

## FIVE



# A GREAT WALL OF WATCHERS

Via social media profiles, we already have many opportunities to curate idealized versions of ourselves. This chapter explores visions of a possible future in which nation-states mandate curation of the ideal self via a system of punishments and rewards—making moral judgments about the appropriateness of our information—as viewed through China’s experimental Social Credit Score system. It examines our own messaging practices in the West, starting with our earliest profile-building practices on Facebook, asking what our networks of connection and our information-sharing practices say about our needs as both individuals and societies.

We may not admit it, but most of us likely get a tiny thrill when we notice that someone has “liked” a comment of ours on Facebook, retweeted a Twitter post, or “hearted” an Instagram photo. These small acts of validation can go a long way toward not only showing our friends and acquaintances what we approve of, but—in China, at least—showing the government who the “good citizens” are. In what sounds suspiciously like an episode out of the British science fiction television series *Black Mirror*, China is in the process of unrolling what’s colloqui-

ally called the “Social Credit Score” (SCS).

The premise is simple: the more likes, retweets, and hearts you get on your social media profile from “good citizens,” the more rewards you will gain in the form of desirable services—everything from expedited travel permits to bank loans. Unveiled in 2014, the Chinese government’s proposal, titled “Planning Outline for the Construction of a Social Credit System,” called for the Social Credit Score to be fully implemented nationwide by 2020.

It’s not hard to imagine how it would work. While in the West we are relatively free from governmental oversight of our social media activities, net states routinely collect data on who likes what content on our profiles (how many likes or retweets or hearts we get), what we spend our money on (through our purchase history), our whereabouts (using cell tower data, regardless of whether we “check in” or even whether we opt out—as recently admitted by Android),<sup>1</sup> our health (for Fitbit or other wellness app users), and so on.

While net states’ goals for this monitoring include, among other things, to better target users with ads, China’s goal with the SCS is explained by the Chinese government as serving loftier ends. According to official documents, the SCS—already in use in parts of China—will enhance “trust” nationwide and build a culture of “sincerity.” The plan goes on to say that the SCS will “forge a public opinion environment where keeping trust is”—and this is the government’s word, not mine—“glorious.” Finally, the SCS will purportedly “strengthen sincerity in government affairs, commercial sincerity, social sincerity and the construction of judicial credibility.” By punishing citizens who get a low score and rewarding those who score high, the SCS will make everyone *want* to be better citizens. Thus it will be easier to trust everyone, as people will simply *be* better citizens—never mind that they’ve been *forced* to become better citizens.

Or are they? Are Chinese citizens *compelled* to use social media? Are any of us?

There’s a saying in Chinese: Rén pà chūmíng zhū pà zhuàng (人怕

出名猪怕壮), which means, “People fear fame like the pig fears being fattened for the slaughter.” In other words, greater visibility comes at a cost; fame has its price.

Nowhere is this more apparent than in China’s implementation of the Social Credit Score. As a person’s online profile grows in visibility, so too does the data that feeds his or her Social Credit Score: a ranking of how “good” a citizen that person is.

The SCS works much like a financial credit score. Having no credit history is almost as problematic as having a bad credit history, as banks have no information by which to assess your reliability as a debtor. With the SCS, rather than assessing your financial reliability, they’re assessing your reputational reliability.

In the United States, if you have a “good” financial credit score, you’re more likely to be approved for a loan by a bank. In China, if you have a “good” SCS, you’re more likely to be approved for a myriad of services; yes, economic services like loans, but much more than that, as we’ll see.

So what exactly are the actions that will improve or destroy a person’s SCS? Given that the SCS is being implemented among the largest online population on Earth, it’s surprisingly difficult to obtain a precise list of offenses that will damage one’s SCS or smiled-upon activities that might give it a boost. When the initiative was announced in 2014, the Chinese Communist Party (CCP) cited four categories for evaluation: “commercial sincerity,” “social security,” “trust breaking” and “judicial credibility.”<sup>2</sup> But what these categories translate to in action is much harder to discern. As noted on the previous page, social media activity is crucial (both what one posts and how others respond). Beyond that, though, all we have to go on is anecdotal evidence. And from what that tells us, the SCS reaches into every nook and cranny of a person’s digital existence.

We have a few recent examples of what’ll get a person’s SCS dinged: In March 2018, 9 million people with “bad” credit scores were banned

from purchasing plane tickets. An additional 3 million travelers were denied business-class train tickets, despite the fact that they had the money for them.<sup>3</sup> Their offenses? In some cases, there had been pretty clear-cut infractions, such as attempting to board the train without a ticket or smoking in a nonsmoking area. But deeds that appeared to be borderline benign or, at the very least, difficult to clearly define—loitering, for example—also contributed to a bad SCS. In one case, a Chinese lawyer was barred from buying a plane ticket because a court-ordered apology—which he had in fact turned in, in writing—was deemed “insincere.”<sup>4</sup>

A person’s spending habits are subject to rating by the SCS as well. Pay bills late? Lose points. “Waste” money on “frivolous” purchases? Lose points.

How wisely a person spends time is also subject to evaluation. Spend too much time playing video games? Lose points. Spread “rumors” on social media? Definitely lose points.

But does all this really matter? What impact might the SCS have on a person’s day-to-day life? Well, a low score might mean that your kids could be denied access to certain schools, regardless of their grades or other qualifications, or you might be banned from travel.<sup>5</sup> If you have a bad score long enough, you might be put on a government blacklist, which could keep you from getting a job.<sup>6</sup>

Conversely, with a high score you might get enhanced book-borrowing privileges at the local library and, on a rainy day, a loaner umbrella.<sup>7</sup> You might improve your chances of securing a mortgage, enhancing your likelihood of financial stability, which in turn could make you a more desirable mate. This is reflected in the practice of those with a good SCS being featured more prominently on China’s largest dating site, Baihe. “A person’s appearance is very important,” said Baihe’s vice-president, Zhuan Yirong, to the BBC. “But it’s more important to be able make a living. Your partner’s fortune guarantees a comfortable life.”<sup>8</sup> You also get to enjoy the incalculable gains of knowing that *other* people know you are considered “good” in the eyes of the government.

Clearly, there are several problems here, the overwhelmingly obvious one being this: What criteria are being used to decide what's "frivolous"? What's a "rumor"? What makes an apology (a *court-ordered* apology, remember) "insincere"? There doesn't appear to be a nationwide set of rules or standards for how the SCS is to be implemented. In other words, some officials within a certain branch of the Chinese government decide what's frivolous or a rumor or what makes an apology legit, but nowhere does anyone share these decision-making criteria with citizens, nor are the criteria uniform across the country. You just have to *hope* that your actions don't piss off the SCS monitors, learn from your neighbors, and be frequent but vigilant in your social media activity.

In some places in China, the incentive is especially high: citizens with a good SCS get a special shout-out from certain local governments. In one of the three dozen cities where the SCS system was first piloted en masse, a midsize city called Rongcheng, photographs of citizens with a good SCS were displayed on public bulletin boards in the town square under a banner that read: "Civilized Families." (Check *Foreign Policy* magazine's excellent feature on the SCS for pics of this.)<sup>9</sup> And in Rongcheng, the oversight authority for the SCS has devised a mathematical approach for managing the SCS of its 740,000 adult citizens, potentially lessening uncertainty. According to interviews with officials conducted by reporter Simina Mistreanu, each Rongcheng adult citizen starts with 1,000 points. You gain or lose points depending on your behavior. Traffic ticket? Minus 5 points. Do a "heroic deed," help your family "in unusually tough circumstances," or conduct "exemplary business"? Plus 30 points. Win an award at work? Another plus 5. Whether this rubric is shared publicly with the citizens of Rongcheng is unclear, nor is it apparent whether other cities are using the same criteria. But at least there's a discernible pattern here: Do good stuff and you will be rewarded. Do bad stuff and you will be caught—and because your every online action is tracked, chances are you *will* be caught . . . and penalized.

Given what seem to be rather draconian oversight measures, it's surprising to learn that the SCS does actually seem to be increasing trust among citizens, just as designed.

"I feel like in the past six months, people's behavior has gotten better and better," reported a resident of Rongcheng to *Foreign Policy*. "For example, when we drive, now we always stop in front of crosswalks. If you don't stop, you will lose your points."

As counterintuitive as this may seem to Westerners, whether it's out of fear of losing points or the desire to gain points, the SCS seems to indeed be welcomed by at least some Chinese citizens. According to an interview with Rachel Botsman, who recently wrote a book on the SCS, "When I interviewed people from China on this, they don't necessarily see this as a bad thing."<sup>10</sup>

To understand why this might be, it's helpful to know a little about the history of China. In the 1950s a national development plan was launched, led by Mao Zedong, called the "Great Leap Forward." It brought massive upheaval to the country and caused a famine that killed an estimated 15 to 30 million people.<sup>11</sup> This was followed by the "Cultural Revolution" in the 1960s and '70s, when Chairman Mao led the country through a violent social scrub, vilifying members of "Five Black Categories"—namely, rich farmers, landlords, "counterrevolutionaries" who didn't support the communist wave, "rightists," as well as a catch-all class called "bad elements" that included those with high levels of education, such as teachers and "intellectuals."

This era was defined by rampant mistrust: families were torn apart as students—who led the revolution through the youth army, the Red Guards—turned in parents and grandparents for "reeducation" at forced labor camps in the countryside. The Red Army destroyed thousands of temples and antiquities in the name of ridding the country of the trappings of the unjust hoarding of wealth. The country remained in chaos for almost 10 years. Schools and universities were completely shut down from 1966 until 1972. No one studied. No one went about business as usual. Everyone in the country just labored—children and

parents alike.

While the Chinese Communist Party has come a long way since the Cultural Revolution, China's history of surveillance, morality-based punishment, and widespread fear of being "turned in" by even one's own family casts a shadow over at least the elder population to this day. As Botsman reported, "[People] say in their grandparents' generation, [people] knew that the Communist Party had a file on them, but they had no idea what was in that file. This is actually the same system. Digitized, but it's more transparent."

CHINA HAS JUSTIFIED ITS SOCIAL CREDIT SCORE SYSTEM BY POINTING out a very real need: to know who you're doing business with. Brand reputation works that way. For instance, you may decide to spend the extra money on a backpack from L. L. Bean rather than buying some knock-off brand because you know it will likely hold up for a while; the company has a reputation for quality products. In China, as described earlier, mistrust has been a societal issue for decades. And in the absence of a strong legal system, it's difficult to hold people with shady business practices to account. With the SCS system, in theory everyone knows how reliable everyone they're engaging in business with is, and therefore consumers have the means to protect themselves against less than honorable purveyors of goods and services.

Such a system is easier to enforce in China, with its population engaging in the most mobile transactions in the world, than it would be in many other countries. In a ten-month period of 2017, mobile payments amounted to \$12.8 trillion in China, outstripping the United States' \$42 billion in mobile transactions by "lightyears."<sup>12</sup> While this was largely attributable to city dwellers, the diffusion of smartphones among the massive rural population contributed as well; rural folks are leapfrogging straight from cash to mobile payments, without ever having had a checkbook or credit card. The cash-based population with no bank account—estimated by the World Bank to include around 21 million

people in China—went from being under-the-mattress savers to players in the digital economy almost overnight.<sup>13</sup>

The problem is, studies show that newcomers to cashless transactions tend to underestimate the damage late payments can do to one's credit. Thus they're more likely to make late payments.<sup>14</sup> Given this, it seems that the 21 million financially inexperienced Chinese now using mobile payments are extremely vulnerable to accidentally damaging their SCS, simply by virtue of being new to the very notion of credit.

Praise of the SCS system by ordinary Chinese for how it “establishes the idea of a sincerity culture,” as the government planning documents put it, is almost impossible to find, with the Western media understandably focused on the Orwellian overtones. But, as noted above, it's important to recall the rampant mistrust that permeated Chinese society for decades. Furthermore, prior to the SCS system, the average Chinese citizen had few means of redress to deal with fraud, corruption, or other bad business practices.<sup>15</sup>

The SCS system may be terrifying to Westerners, and certainly a sound constitution and legal system for the Chinese people would be more just than the less-than-transparent SCS. But to the average Chinese person used to dealing with hucksters and swindlers—*pianzi*, in Chinese—the SCS may make life slightly more manageable—so long as they stay on the government's good side, of course.<sup>16</sup> As China hand Jonathan Margolis wrote in a *Financial Times* op-ed, “I am almost embarrassed to say, I get it. Bearing in mind China's violent history, I understand its preoccupation with order and harmony.”<sup>17</sup> Society would indeed be “glorious” if we could all trust and be trusted.

FACE TO FACE, WE RELY ON A HOST OF VARIABLES TO DETERMINE whether or not to trust someone: their smile; how well they maintain eye contact; their body language; and, of course, their words. Our social networking platforms have far fewer data points to go on. Facebook, for instance, can't (yet) gauge whether someone is exhibiting suspicious

cues such as shifty eye contact or excessive fidgeting. Perhaps it's not surprising to find that they've identified other ways to assess whether we might want to "trust" someone—in other words, to make a person part of our social network. One such way is to determine whether we're already in contact with that person *outside* of Facebook.

And such a determination *is* made.

"Creepy. Phoned a guy on mobile after he gave me his number in the weekend at the retro caravan show (first time I have met him). Today @ Facebook serves him up as People you may know. We have no mutual friends so Facebook is looking at my phone call history. Intrusive?"<sup>18</sup>

This tweet reflects one of the many practices that Facebook has taken heat for in the past few years: the "People You May Know" feature. Just who gets served up reveals how extensive and detailed Facebook's profiles are on its users. First off, your profile includes anyone stored in your phone's contacts list.<sup>19</sup> In addition, Facebook also stores your connections to "shadow profiles"<sup>20</sup>—detailed accounts about people you interact with who've never signed up for Facebook.<sup>21</sup>

The public reaction to learning about these practices was, predictably, outrage. This was followed by a small wave of folks fleeing to Instagram (which, perhaps they didn't know, Facebook also owns).<sup>22</sup> Yet despite the public pie-in-the-face that Facebook has taken in the last two years for these practices, along with scandals like Cambridge Analytica, the platform remains extremely popular, especially outside the US.

Almost 2.2 billion people use Facebook across the globe. US engagement rates on Facebook have declined, but worldwide adoption climbs steadily each year.<sup>23</sup> Even among those who are less engaged with Facebook now than in the past, the site remains a staple of the digital experience. It's so popular that in many countries, Facebook is almost synonymous with simply going online. "It seemed that in their minds, the Internet did not exist; only Facebook," recalls one researcher who studied internet use in Indonesia.<sup>24</sup> Indeed, 11 percent of the 94 million Indonesians using Facebook reported that they did not use the internet but *did* use Facebook. In their minds, Facebook *is* the internet.

To understand why Facebook remains so popular despite its flaws, it's worth remembering what Facebook gave us—and continues to give us. Facebook gave us the first digital space—the first space anywhere, for that matter—where absolutely anyone could create an idealized version of themselves. Once satisfied, they could then share that with a handpicked collection of other people.

Prior to Facebook, only the very famous could curate their public persona, via expensive public relations firms; and even they couldn't control bad news about themselves. Facebook gave rise to the curated self: a place where you could amass and flaunt the most complimentary photos, issue the most modestly worded self-congratulatory posts, share the most aren't-I-smart-and-socially-conscious news stories. And you got to pick who would see all of this—in other words, create your very own collection of fans. Any random thought, quip, joke, observation about your day, the world, the nature of existence was fair game. What's more, people would reward you for sharing these tidbits—with their likes and comments, and now, with a whole range of emoticons designed to validate your musings.

Even given this somewhat cynical take on what Facebook does to one personally, it's impossible to discount the incredible influence it's had (and has) on the world socially. True, grassroots social protests have always spread from person to person—from individual friends to extended family members to neighborhoods to communities. But with Facebook's network effects—where the more people who are part of a network, the more powerful it becomes—movements have the capacity to hit the public consciousness with the force and speed of a hurricane.<sup>25</sup>

Social movements, energized on Facebook, become simply inevitable. You may not join the movement yourself, but you will see something about it; know of its existence. Think #MeToo: more than 12 million people posted with this hashtag on Facebook within the movement's first 24 hours.<sup>26</sup> Think #BlackLivesMatter: over 3 million people watched the shooting of Philando Castile on Facebook Live the day it happened.<sup>27</sup> Think #ArabSpring: the five days of protests in Cairo that toppled the

almost-30-year reign of President Hosni Mubarak were organized on a Facebook page.<sup>28</sup> Even if you don't know what these hashtags represent, chances are you've at least come across them. And even greater are the chances that you did so on Facebook.<sup>29</sup> I teach a class called "Technology, National Security, and the Citizen" at Columbia University, and I asked my students in February 2019 how many of them were on Facebook. Everyone raised a hand, if somewhat sheepishly. As one student commented, "Even if we *wanted* to stage a mass exodus from Facebook, where would we organize such a thing? Yep—on Facebook."

Whether you're on it or not, for good or for ill, Facebook helped define the past decade of the digital age. While Facebook the net state may someday perish, its innovations have already influenced the next generation of programmers and engineers. Politicians too. And countries with one-party political systems, like China. There would be no Social Credit Score without Facebook, because there was no such thing as a digital social network *before* Facebook. Though by 2019 many Americans have lost their faith in Facebook, it's impossible to deny the influence that Facebook has had over the past fifteen years, shaping a generation of social interactions, political movements, and personal acts of identity-curation.

JUST BECAUSE AN AMERICAN TECH FIRM CREATED THE SOCIAL NETWORKING phenomenon doesn't mean that it could give rise to an American version of the Social Credit Score system, right? We do have the US Constitution, the bedrock for law and order in the United States, which seems to stand in the way of a China-like Social Credit Score taking hold here. But aspects of the SCS system and its related technologies have gotten the attention of Western governments and net state leaders alike in ways that we should pay careful attention to.

Let's start with facial recognition. For the SCS, associating a person's face with a name is in many ways just another data point: Can we access person X's buying habits? Check. Do we know people's social media

handles so that we can track their behavior online? Check. Can we identify who's jaywalking and instantly send them a fine via text message? That's a check, too. In Shenzhen, an industrialized city bordering Hong Kong, China rolled out a facial recognition program to do just that back in March of 2018.<sup>30</sup> With 170 million surveillance cameras already in place countrywide and plans to up that total to 570 million by 2020, the CCP will soon be able to devote one camera for every two citizens to track when they board and leave the subway, verify student identity for school tests, even dispense toilet paper to ensure that no individual takes more than their allotted two sheets.<sup>31</sup>

But again—that's just in China, right, where citizens' rights are somewhat nebulous? If only we could claim this with confidence. Other countries and net states are paying close attention to how this mass surveillance pans out in China, with an eye toward importing it for use closer to home.

Germany, for instance, is purported to have modeled its facial recognition pilot program at Berlin's Südkreuz train station after the Chinese system—and it was recently extended for further data collection, despite protests by German citizens over privacy concerns.<sup>32</sup> China outright exported its facial ID technology to Zimbabwe, although CloudWalk, the company that manages the facial recognition technology, insists that it was sort of an add-on: "The Zimbabwean government did not come to Guangzhou purely for AI or facial ID technology; rather it had a comprehensive package plan for such areas as infrastructure, technology and biology," according to CloudWalk CEO Yao Zhiqiang.<sup>33</sup>

American net states are keeping an eye on developments in China as well. For the first time ever, China's World Internet Conference—formerly described in the *New York Times* as a rather dinky affair attracting "local tech execs and leaders of impoverished states"—in 2017 managed to secure the attendance of some of the major net state players, including Apple CEO Tim Cook and Google CEO Sundar Pichai.<sup>34</sup>

The focus of the conference? China's surveillance state.

At the conference, Face++, one of the fastest-growing Chinese facial

recognition companies, displayed a demo in which they surveilled the conference attendees, then broadcast from their booth how they could identify individual attendees' gender, hair length, color, and even clothing. Another exhibit showed off a map of Beijing that pinpointed every single foreigner in the city, using surveillance footage and GPS data from their cell phones.

The American tech industry isn't stopping at mere observation of China's surveillance state: it's betting on its success with investments. A report by Reuters identified three primary companies in China's mass facial recognition surveillance triumvirate: SenseTime, DeepGlint, and Face++.<sup>35</sup> All three companies, according to that report, are recipients of significant funding from Silicon Valley venture capital firms. Sequoia Capital, one of the largest venture capital funds in the Valley, has made 206 investments in China since 2000, including an \$18 million investment in DeepGlint in June of 2018. Another major Silicon Valley venture capital firm, Silver Lake, was one of eight lead investors in SenseTime.<sup>36</sup> And the artificial intelligence venture capital fund Comet Labs' very first investment back in 2013 was in Megvii—better known as Face++, China's biggest facial recognition software firm, which is now valued at roughly \$1 billion.<sup>37</sup>

It matters that the American tech industry is aiding China's surveillance program, because by any account the program is anything but benign. It's being used to target specific populations—not because of criminal activity, but because of suspicion that these populations *might* someday engage in such activity. The most extreme example of facial recognition targeting is in China's westernmost region, Xinjiang—one of the so-called autonomous regions. The ethnic minority native to Xinjiang, the Uighurs, are undergoing what might be the world's most intensive surveillance-state experiment to date.

Using some Uighurs' involvement in past protests as an excuse, China was able to justify a comprehensive tracking system for the minority group as a national security measure. But regardless of the justification, the measures are extreme: according to a grim op-ed by historian

James Millward,<sup>38</sup> every 100 feet Uighurs pass police checkpoints at which police scan their ID cards, irises, and cell phones. Using sophisticated facial recognition software—which works well to distinguish Uighurs, who have different physical features than Han Chinese—the government has built a vast database of the roughly 11 million Uighurs, a feat that would have been impossible before the advent of AI surveillance.<sup>39</sup> Even routine purchases by Uighurs that might be considered threatening, such as buying a kitchen knife, are logged in databases. In the city of Aksu, shop owners are now required to etch the buyer's name and ID number into the blade of any knife a Uighur buys with a QR code tied to that buyer's name, a policy “intended to trace a knife back to its owner in the event it's used to commit acts of violence,” as reported by Radio Free Asia.<sup>40</sup>

While no state in the US has yet to roll out a comprehensive suite of tracking and facial recognition tech such as that in Xinjiang, there aren't any laws on the books prohibiting it. As noted in the previous chapter, Microsoft recently issued a statement calling on Congress to institute some sort of regulation for facial recognition technology.<sup>41</sup> “Advanced technology no longer stands apart from society; it is becoming deeply infused in our personal and professional lives,” wrote Microsoft president Brad Smith. “[The] potential applications are . . . sobering. Imagine a government tracking everywhere you walked over the past month without your permission or knowledge. Imagine a database of everyone who attended a political rally that constitutes the very essence of free speech. Imagine the stores of a shopping mall using facial recognition to share information with each other about each shelf that you browse and product you buy, without asking you first.”

Tech companies aren't known for asking permission before they develop a life-altering product—that would be almost like a teenager asking his parents for *more* rules. Their call for regulation should give us all pause; it's an acknowledgment that the makers of this technology recognize how possible it would be to use it to restrict user liberties.

At the same time, however, many elements of a system to assess so-

cial credit are already in place in the West—largely because of efforts by tech companies and emerging net states. In the United States, almost every adult has a financial credit score, for example. There are other scores out there too—scores assessing intangibles such as reliability and friendliness: anyone who ride-shares with Uber or Lyft, for instance, gets rated by their driver (and vice versa). In addition, everyone with a social media presence is *connected* to people with either good or bad credit scores and good or bad Uber or Lyft ratings—connections that would count in China. But these numbers aren't readily available to the public except on a site-by-site basis.

Which is ironic. In the West, private corporations like data brokers can see our *compiled profile* of rankings. But we, as individuals, can't. In China, on the other hand, the government itself compiles the profiles, and while citizens don't necessarily know what will improve or degrade their ranking, at least they can *see* their own profile.

If you took the time, however, you could make a little compilation on yourself. Get your credit score from each credit agency (which you can do for free) and collect your ratings from all your sharing-economy apps—home-sharing services like Airbnb, ride-sharing services like Uber and Lyft. Then assess your public digital footprint by Googling yourself. This wouldn't be just a vanity project—you'd be assessing how others size you up. For instance, if the search turns up a flattering Facebook profile picture, your chances of getting a job interview increase by as much as 40 percent.<sup>42</sup> But don't stop there. Your Fitbit data may reveal how healthy you are; your Amazon purchase history, how lavish you are. Your Google search history may uncover a pattern of queries that are impressive—queries that make you seem socially conscious and inquisitive, for example—or less than flattering—like Google-stalking a new acquaintance or asking about things you're embarrassed that you didn't already know. Indeed, with enough patience and perseverance, you too could create your own version of a social credit score. But even then, you'd still “know” less about yourself than one of the country's five major data brokers, which typically have about 3,000 “data segments”

on every American.<sup>43</sup>

There's another saying in Chinese: *Er tīng wéi xǔ, yǎn jiàn wéi shí* (耳听为虚, 眼见为实). It means, in effect, "Seeing is believing." We apply that saying every day: we trust people we've had a chance to "see," to get to know—or at least we did until the internet made us question what we see. Our ability to craft the perfect version of ourselves with our online profile makes it difficult to know if we can trust the *other* digital personas we encounter. And in an age where we have increasingly frequent interactions with people we've not met in person—work colleagues we communicate with only via email, social media "friends" who don't even live in our country—any proxy for trust could be a big help in discerning who's reliable and who's a sham.

But it's unlikely we'll find a replacement for our own personal assessment. We've yet to find a substitute for good old-fashioned instinct. Our "gut" can help us sniff out a criminal,<sup>44</sup> pick the right romantic partner,<sup>45</sup> or prevent us from making mistakes.<sup>46</sup> We barely understand how the human brain actually works, so we can't replicate it. "We know about connections, but we don't know how information is processed," reflected Stanford University neurobiologist Lu Chen at a lecture on the challenges of neuroscience. "We are still in need of an understanding of the fundamentals," echoed another neuroscientist in attendance, Nobel laureate Tom Südhof.<sup>47</sup>

Until we've got the brain figured out, it's unlikely we'll be able to recreate a copy with the fidelity to replace our deeply felt instincts about whether or not to trust someone. What we *can* rely on net states for are the troves of data that can aid in either confirming or denying whether our instincts are spot on. But so long as we're pheromone-emitting, sub-conscious information-processing creatures, tech (hard as it may try) can't yet replace face-to-face interactions when it comes to establishing trust. China may be creating a centralized database of "trust breakers," but coworkers, neighbors, friends, and family will—one hopes—still establish their own relationships, regardless of what their government or net state rankings say.

FOR ALL OUR CONCERNS ABOUT PRIVACY, WE SEEM TO PLACE A LOT OF trust in our technology, seemingly without a second thought. Take search engines, for instance. It probably doesn't occur to most of us to think of typing in search terms as an expression of trust. And in some ways, it's not—we don't need to have the usual hallmarks of trust (feelings of respect and admiration, say)—for a search engine to proceed, after all. It's a tool; we use it, it gives us answers.

But we trust in the search engine's ability to give us answers—indeed, *right* answers. It's implied in the very fact that we use the tool. In exchange for our trust, search engines do more than give us answers. They give us power. Not just the *feeling* of power, either; actual power—power we could never possess without them. Perhaps this is why we're so willing to trust our personal data, including the most intimate questions that cross our minds, to search engines—to Google, specifically. Because the power we get in return is worth it.

Consider what goes into a search. Each and every query we type into Google Search travels an average of 1,500 miles to a data center somewhere in the world and engages over 1,000 computers, generating a result in 0.2 seconds.<sup>48</sup> This is possible only because Google Search is constantly crawling over 100 billion web pages, then storing and organizing the information found. "It's like the index in the back of a book—with an entry for every word seen on every web page we index," reads Google's blog post on "How Search Works."<sup>49</sup> It's a staggering amount of data, processed extraordinarily fast. And Google Search feeds us remarkably accurate results even if we use poorly worded search terms that the search engine has never encountered before. (Each day, 15 percent of all queries have never been asked of Google before.)

And we ask our questions in increasingly personal spaces: our phones. Ninety-six percent of cell phone owners in the US used their phones for searches in 2019 (with Google handling almost all of those searches).<sup>50</sup> But while Google may help us satiate our curiosity, it's largely thanks to Apple's invention of the smartphone that we can do so at any time and anywhere we happen to want to know something.

This brings us to the question, So what? We find stuff out, fast. And the data we create in the process of finding stuff out is available for us to review, if we want. If we go to MyActivity.Google.com, we can see every search we've ever entered, on any device, since we created an account however many years ago. We can even download the entire archive so that we can peruse our curiosity profile in our spare time. But if we bothered, what would we find out about ourselves that we don't already know, somewhere in the deep recesses of our minds?

In the book *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are*, data scientist Seth Stephens-Davidowitz traces the fascinating history of how we tend to fool ourselves, especially when reporting on our behavior to others. Surveys—one of the most common social measurement tools in use—are particularly problematic. People tend to overestimate their positive attributes and downplay the negative when reporting on their own actions (even when doing so anonymously), an effect called the “social desirability bias.” Studies suggest that people self-report eating less, being more physically active,<sup>51</sup> voting at higher rates,<sup>52</sup> drinking less alcohol,<sup>53</sup> being more (for men) or less (for women) sexually active,<sup>54</sup> and giving to charity and volunteering,<sup>55</sup> to name just a few.

And we don't just pretend to be better people to other people; we fool *ourselves* into thinking we're generally better and, specifically, smarter than we actually are. In what's known as the “Dunning-Kruger effect,” everyone from students to long-serving professionals overestimates their intelligence and abilities. In a *Forbes* profile on this effect, the author cites studies showing that 32 to 42 percent of software engineers rated themselves as being in the top 5 percent of performers in their companies.<sup>56</sup> A nationwide poll conducted by CNBC revealed that 20 percent of Americans thought it was “fairly likely” they'd be millionaires within the next decade<sup>57</sup> (while only 10 percent of all Americans actually *are* millionaires). Take the fact that we think we're smarter than we are in general and combine it with the fact that search engines make us feel smarter still, and we've got a fairly unrealistic—and inflated—sense of

self on our hands.

What makes us so bad at estimating our own abilities and predicting a realistic future? The answer lies, in part, in confidence—or rather, overconfidence. It's not something we can help; overconfidence in our abilities is an innate bias, built in and hardwired. It makes sense on some intuitive level: if we believe in ourselves, we're more likely to try difficult things. Imagine the opposite bias: underconfidence. We'd never have tried anything hard and would likely never have made it very far as a species. Indeed, researchers believe that there's an evolutionary advantage to overconfidence: it rewards people for stretching themselves to the limits of their abilities. Perhaps they won't achieve their original goal, but they'll certainly be better off than if they hadn't bothered trying. Overconfidence is also linked to increased morale, to persistence, to the ability to project credibility, and to creating self-fulfilling prophecies.<sup>58</sup>

The problem is, overconfidence also leads us to wildly underestimate how difficult tasks are and how powerful our foes or challenges are. Overconfidence bias has been linked with historically cataclysmic events ranging from World War I, the Vietnam War, the first Gulf War, the 2008 financial crash, and the federal government's underpreparedness for natural disasters such as Hurricane Katrina.<sup>59</sup> Ironically, the more expertise we have in a given area, the more susceptible we are to the overconfidence bias. Cultural norms also come into play. It's probably not surprising to learn that men exhibit overconfidence more often than women, who are culturally encouraged from girlhood on to be accommodating rather than assertive with their opinions.

This matters because if we aren't honest with ourselves about our own abilities, we pursue goals that are simply not realistic. This both sets us up for failure and causes us to waste time that could be better spent on endeavors more closely matched with our actual abilities.

Getting around this is pretty tricky. Because to know what competence looks like—how good you have to be to achieve a goal—tends to require actually *being* competent already. As a result, being unable to do

something at a level of excellence means that you can't really imagine what it would take to *be* excellent at it. Think about something basic, like riding a bike. To look at the process from the outside, it's straightforward. It looks like you just get on the bike, pedal, and you're off! But as any of us who've learned to ride a bike might recall, it's nowhere near that simple. There's the issue of how to balance before you pick up speed, how to pick up speed from a standstill, how to steer while also picking up speed, and how to do all these things in concert without crashing into anything. Like most easy-looking things, bike-riding involves multiple steps to achieve even basic competency, let alone mastery. In other words, we tend to look at things that *look* easy as being, well, easy to do. And this is another reason why we overestimate our ability to be good at things. Until we *experience* mastery, we simply can't fathom how hard it is to get there.

This relates to search engines in two ways. First, online searches can make us feel like geniuses; with Google, we're all information-finding ninjas. We've already established that we tend to feel more powerful and more intelligent thanks to Google Search, even when we're unsuccessful at finding what we're looking for—after all, we have this incredible processing power working to augment our brain's ability to find the answer to something. Second, online searching feels anonymous, perpetuating our ability to lie to ourselves about what we really want and thus who we really are.

Here's where data collection once again comes into play. As you do general web browsing and searching, your computer is collecting data on what websites you visit, and the content on specific pages, and sending that information back to the host website. Ever notice how you might be shopping for shoes one morning and then, later that day, you get an ad for the same shoes on Facebook or Gmail? This is a reminder that our activities, while they might feel anonymous, are in fact tracked. Even when we enter into "incognito mode"—Google Chrome's "private" web-browsing option—while the web browser doesn't track your history or

the content of the sites you visit, your ISP (internet service provider) certainly does. In short, you can't access the internet without letting at least the entity that's providing you with a connection *to* the internet see what you're searching for.

As we use search engines, we're fueling our innate sense of overconfidence, empowered by the sense of intelligence we get by getting answers to our queries so damn fast. Imagine what this does to us, as a people, on a global scale. If on average, 57 percent of the population of Earth does a search on Google at least once a day, then once a day 4.2 billion people get a little cognitive boost. This boost makes us slightly more overconfident in our intellectual abilities—a problem we already struggle with, thanks to our innate overconfidence bias. We feel empowered, smarter, and as a consequence, take greater risks; we overestimate our abilities to succeed.

If one of the goals of being human is to know oneself, search engines both help and hurt us. They allow us to find out all kinds of things we might never know otherwise. But at the same time, they fuel what is ultimately an unrealistic view of ourselves and our abilities. Search empowers us, but in so doing it further obscures our sense of reality. To know ourselves, then, maybe we need to look further inward for answers and rely on search engines a little less.

ULTIMATELY, ALL OF THIS SHOWS WHY RELYING ON NET STATE DATA AS the primary means to assess a person's worth is a problem. Net states—and nation-states, such as China, engaged in digital monitoring—know only *versions* of us: the idealized self that we curate for Facebook; the frustrated self that we reveal in what questions we seek answers to on Google; the hyperconfident self that posts clever reviews on Amazon; the isolated self that unlocks our iPhone 63 times a day, hoping for something, anything, to distract us from our loneliness.

We're infinitely complicated creatures, inhabiting multiple and of-

ten contradictory versions of ourselves all at once. A national scoring system (like China's Social Credit Score) that assumes it can know people based only on their digital footprint is dangerously naive; it's like taking a person's photograph and then claiming knowledge of their soul.

Governments will never be able to fully know their citizenry—not even China's rapidly developing surveillance state. The danger with systems like the SCS is that they *assume* they can—and with a high enough degree of confidence that they act on that assumption, sometimes harming people's physical and interior lives.

One last proverb. It goes something like this: To know a man, look only to his friends. To know a king, look only to whom he employs. “The wise man,” it concludes, “is exceedingly careful about the company he keeps” (君子慎所藏).

Here's the thing: the company *I* keep, personally—and I suspect many of us—isn't, for the most part, kept online. For instance, I don't think I've ever exchanged Facebook messages, comments, or likes with my husband; not my brother or my best friend; *certainly* not with my kids (they'd be mortified). I rarely even send any of those people emails. That's because, despite all the evidence of my life online, I still live the majority of my life offline. Most of us do. Even with our eyeballs on screens hours upon hours a day, we still have to reside someplace physically and interact with neighbors. We have to go to work and converse in person with colleagues, or go to school and engage with our teachers. We see friends. We have experiences—all offline.

Thus, any government mapping of our worth based on our digital footprint alone overlooks the most important data points about us: the vast majority of time we spend living life when *not* on tech. Our digital reflections may be highly sophisticated renderings of the self we want the world to see, but they're not trustworthy stand-ins for the real person—not yet.

## SIX



# THE ALL-KNOWING INTERNET OF THINGS

Tech is increasingly personal, collecting data on our individual behaviors whether we're aware of it or not. This chapter explores our daily life with technology, examining the tech we use in our homes and our public spaces with the so-called internet of things (IOT) and how the IOT currently influences and is likely to affect our daily existence. It looks at developments in user profiling, starting with Amazon's recommendation system and "smart" technologies such as Amazon's Echo that gather data on our health, our environment, the information we seek, the music we play. It tackles the question of whether these practices let our net states "know" us, and whether, ultimately, users have any say in the matter.

If you Google the phrase "What is the internet of things?" in 2019, you'll still find explainers and primers: "What Is the Internet of Things? A Complete Beginner's Guide" (*WIRED*); "6 Things Everyone Needs to Know About the Internet of Things" (Business Insider website); "The Internet of Things: Could It Really Change the Way We Live?" (*The Telegraph*). That's how new it still is. In 2014, a much-cited Accenture poll reported that 87 percent of people had never heard of the internet of

things.<sup>1</sup> Five years later, that's transformed from "never heard of" to—apparently—"Don't really understand."

Incredibly convenient, the internet of things is arguably also the greatest threat to individual privacy to date. It includes lots of things. Internet-enabled household devices, like coffee makers, refrigerators, and televisions. Internet-linked wearables, like smart watches and Fitbit-type health trackers; voice-enabled assistants, such as Apple's HomePod, Amazon's Echo, and Google's Home; as well as smartphone apps we keep tethered to our physical health, like heart rate monitors and step counters. Computer-assisted cars. The smart thermostats that regulate our air conditioning and heating. Our cloud-based home security systems.

Soon, the internet of things will include anything you can stick a sensor on: in 2018, scientists developed a thin-film electronic sensor—an internet-enabled sticker, essentially—that could conceivably turn *any* object into an IOT device.<sup>2</sup> "We could customize a sensor, stick it onto a drone, and send the drone to dangerous areas to detect gas leaks, for example," said Chi Hwan Lee, Purdue assistant professor of biomedical engineering and mechanical engineering, one of the scientists who created the device.<sup>3</sup> Or, for example, you could stick this sensor on a flower pot, suddenly enabling the pot to detect temperature changes that might affect how the plant grows.

According to the phone giant Ericsson, there were more IOT devices in 2018 than the world's 7.4 billion mobile phones.<sup>4</sup> Other industry experts predict that this number will increase to 30.7 billion by 2020 and 75.4 billion by 2025. Here's another way to look at it: by 2020, there will be an average of four IOT devices per person on the planet; by 2025, that will increase to nine devices per person.

Considering that most of us aren't even aware of how many IOT devices we have in our vicinity, this is a disconcerting thought. Because smart devices talk to each other, an IOT doesn't necessarily require our intervention to work—which is exactly the point.

This raises the question of what the IOT industry means for our abil-

ity to exert control over our data and our identity. Opting out of the IOT doesn't appear to be an option moving forward. When polled by Pew Research in 2017, industry experts almost universally concluded that despite a certain creepiness factor inherent in the IOT, it would indeed be adopted by almost everyone, either because "the magical behaviors that the new devices will provide will be too strong for people to resist" or because "a significant number will have the illusion of being disconnected [when they actually are not]."<sup>5</sup>

Since an IOT device doesn't necessarily require user intervention to function, once we set it up it's entirely possible to forget that it exists. The technology, like so many other technologies, may seem magical at first, but it quickly becomes invisible to users—both the tech itself and the implications of what net states do with the data they collect from IOT devices.

The marketing term for internet of things products—"smart" devices—is not entirely accurate: they're less smart than just chatty. They're in near-constant communication with their manufacturers, checking for updates and sending notifications that they're still functioning.<sup>6</sup> Smart TVs, for instance, track and report back to their manufacturers on what you watch, for how long, and how often. But they also connect with the other internet-enabled devices in your home—your phone, your laptop, your smart thermostat, your smart door-locking system—anything using the same internet connection as your television.<sup>7</sup> Given that 45 percent of American homes currently house smart TVs, this generates a tremendous amount of data about a public that remains largely unaware it's happening.

In a chilling experiment to discover what it's like to live in an IOT-connected home, Gizmodo reporter Kashmir Hill converted as many of her devices as possible into internet-enabled ones: this included her Amazon Echo, light switches, coffee maker, baby monitor, kids' toys, vacuum, television, toothbrush, and (to monitor and report on sleep patterns) even her bed. "This must be what it's like to be in a documentary or in a reality TV show," she wrote.<sup>8</sup>

Hill reflected on two disturbing trends. First, she quickly stopped noticing the devices in her home. Being surrounded by internet-connected gadgets became normal—just part of the background. When she stopped to think about it, this lack of awareness troubled her: “If homes become sentient, and it becomes the norm that activity in them is captured, measured, and used to profile us, all of the anxiety you currently feel about being tracked online is going to move into your living room.”

The second disturbing trend Hill noted in IOT-connected homes is the data collection power of the ISP, the internet service provider. Not only do individual internet-enabled devices send data to their manufacturers, but a person’s ISP—Comcast or Verizon or whatever company is paid for internet access—scoops up all that data, too. While in some ways, the ISP is just a utility, like the electrical station that supplies power to a home, it’s also a data sieve. Think of it this way: any data that comes into your home via the internet (your TV shows, your email, the websites you visit) and any data that gets sent out from your home via the internet (your search history, your web-browsing patterns, your purchase requests) goes through your ISP, which acts like a giant screen through which all data traffic flows and gets captured; like a toll collector between your home devices and your destination, whether it be Amazon or Google or Facebook, with your data being the payment that your ISP collects.

And ISPs are now permitted to sell that data. In 2017, Congress passed a bill repealing restrictions on ISPs selling customer browsing and app usage data without seeking individual users’ consent.<sup>9</sup> Whom can they sell this information to? Anyone who wants to pay for it, really. At the very least, though, this likely includes data brokers.

Also, it’s worth bearing in mind that all digital data is leakable and hackable. In June 2018, for instance, the marketing firm Exactis was called out for having publicly exposed its database of 340 million records containing people’s personal information. The records included details ranging from phone numbers and email addresses to the number, age, and gender of a person’s children. “It seems like this is a database

with pretty much every U.S. citizen in it,” reported security researcher Vinny Troia in an interview with *WIRED*.<sup>10</sup> “I don’t know where the data is coming from, but it’s one of the most comprehensive collections I’ve ever seen.”

That a company like Exactis has this much data on us is noteworthy for two reasons. First, Exactis isn’t exactly a household name. Likely, most of us have never heard of it. The only reason it even merited a news story is that it screwed up. This, though, leads to an inevitable question: How many other marketing firms out there have data profiles on us that we *don’t* know about? NSA consultant Edward Snowden shocked the world with his 2013 revelation that the US government ran a program, PRISM, to collect data on American citizens. Yet Americans are somehow less shocked at the prospect that unknown multitudes of market research firms likely have far *more* information on us.

We are, as a people, increasingly distrustful of government. Our confidence in our government has been declining since the 1950s and now rests at rock-bottom historic lows: only 18 percent of Americans report trusting government, down from 77 percent in the 1960s.<sup>11</sup> We don’t trust the people who run our country with our private information—though these are people we have the power to elect or reject—but seem resigned to having no power over net states’ possession of our private information. Even Facebook, whose credibility took a historic walloping in 2018, still enjoys a 49 percent trust rating from its users. While this is pretty low on an objective scale, it’s practically off the charts when compared with our government: the last time 49 percent of Americans trusted their government was 1972.<sup>12</sup> The US Congress, with its 11 percent trust rating, could only dream of Facebook’s 49 percent.<sup>13</sup>

Even with our middling trust rating in Facebook, we’re still on it, en masse. Sure, we’ve directed outrage at this particular net state, hauling its founder, Mark Zuckerberg, before Congress for a good, old-fashioned grilling. But we haven’t given up our allegiance to it or the other net states. (Remember: it’s not just Facebook—*all* our net states engage in data sharing; it’s a core element of their business models. Facebook just

happened to be the one in the hot seat in 2018.)

The data that shapes our individual profiles will only increase as we move from wearing internet-enabled devices, as with phones, to installing them in our homes, as with smart TVs, to having them baked into the very infrastructure of our environment, as with smart cities. Smart city technologies are already being deployed, and in plain sight, but likely to our utter obliviousness.

It's easiest to observe the implementation and grasp the possible implications of smart city tech in an extreme example. Let's take a look at a smart city that's being built from scratch in our neighbor to the north.

CANADA DOESN'T TEND TO COURT CONTROVERSY. IT'S A PLEASANT, polite place that plays by established norms and rules.

Quayside could change all that.

In the summer of 2018, Google's sister company Sidewalk Labs (also owned by Alphabet)—which declared its mission to be “reimagining cities to improve quality of life”<sup>14</sup>—embarked on its first actual foray into city-building. In partnership with a government-funded corporation called Waterfront Toronto, Sidewalk Labs will convert Quayside, a 12-acre stretch of waterfront property, from what locals describe as “blighted, underutilized, and contaminated” into a fully smart city.<sup>15</sup> According to Sidewalk Toronto, as the joint initiative is called, they'll “combine forward-thinking urban design and new digital technology to create people-centred neighbourhoods that achieve precedent-setting levels of sustainability, affordability, mobility, and economic opportunity.”<sup>16</sup>

The ultimate vision is something like a city version of your iPhone. Sidewalk will provide the infrastructure, similar to how Apple provides the iPhone itself. The iPhone apps—what makes the phone interesting—are all designed by third-party developers: Facebook and AccuWeather and the like. Sidewalk's Quayside will have features that are likewise customizable: “If you think of the city as a platform and design in the

ability for people to change it as quickly as you and I can customize our iPhones, you make it authentic because it doesn't just reflect a central plan," Rit Aggarwala, the executive in charge of Sidewalk Labs' urban-systems planning, explained to *MIT Technology Review*. "It also reflects the people who live and work there."

This is where Sidewalk Toronto emerges as an intriguing test case. The 196-page "vision document" that Sidewalk Labs presented to Toronto proposed razing the 12-acre property and creating their city of the future from scratch. The plans include a self-contained geothermal grid to recycle energy, which can then be used to both heat and cool buildings. The city's carbon emissions will be negligible, since cars won't be permitted—only emergency vehicles and driverless transit shuttles. Sidewalks will be kept clear of snow with built-in melters—a must, considering that walking and cycling paths will form the primary arteries for people to get around. Buildings will be constructed from recycled materials, the city will employ smart waste disposal systems, and so on.

Quayside will also be populated with sensors—many, many sensors. They're billed in the vision document as a "digital layer" that covers all aspects of the city. Built into every facet of the neighborhood, the proposed digital layer—read, "IOT, everywhere"—will provide "an unprecedented degree of insight into the physical environment."<sup>17</sup>

That such technology will permit an unprecedented degree of insight into the inner workings of city life is perhaps inevitable. But what's still up for debate is who owns that technology and who has access to those insights. Public infrastructure—protecting and maintaining the roads, bridges, electrical grid, and other spaces for use by any and all citizens—has typically been the domain of nation-state governments. That this city will be constructed and operated by two corporations—Sidewalk Labs and Waterfront Toronto—raises the question of what remains "public" in this scenario. If Quayside's public sidewalks and parks are permeated by sensors, are they really "public"?

It's unclear what, exactly, Sidewalk Labs and Waterfront Toronto plan to do with the data they collect from Quayside's "digital layer." As

of this writing, the questions of data governance (who has access to the data collected at Quayside), data residency (what country the data will be stored in), and how citizens' privacy will be protected are all still being debated. As Anthony Townsend, a former consultant for Sidewalk Labs, noted in a *Politico* profile on Quayside, the fact that these issues have yet to be worked out spells trouble. "This is the city-level question of our time," he said. "And [the governmental leaders of Toronto] haven't taken the slightest step in trying to even create a vision there."<sup>18</sup>

Quayside is tiny—you could walk from end to end in just eight minutes—but it will be a test case for what a truly smart city, one not just *built with* but *integrated into* the IOT, could actually look like. "This is really a grand experiment, in many respects, that is going to teach not just Toronto but really cities all across the world what the future city is going to look like," Bruce Katz, a former Brookings Institution official, reported in that same *Politico* profile. "Of course, if you're Toronto, you're the lab."

In some ways, Sidewalk's Quayside is a technical and ideological moonshot: a future-leaning pilot project designed to test the limits of what cities could be, but also an experiment into how people's lives could be lived. This is not a bad thing. Indeed, it invites a kind of "first principles" thinking that net state leaders like Elon Musk have credited for their many successes.<sup>19</sup>

First principles thinking is a concept borrowed from physics. "The normal way we conduct our lives is we reason by analogy," Musk explained in an interview. "[With analogy,] we are doing this because it's like something else that was done, or it is like what other people are doing. [With first principles,] you boil things down to the most fundamental truths . . . and then reason up from there."

This means that instead of looking at how to solve a problem using existing road maps, you start with the very essence of the problem itself, questioning every assumption and every previously attempted solution. Cities are an excellent target for first principles thinking, because they're quite literally built on assumptions.

Case in point: city roads. Most cities' road systems evolved through use. Dirt roads at one point became paved, not necessarily because they were the most direct route from point A to point B but because those were the routes people were accustomed to. Boston is a famous example of this, with its tangled web of streets evolved from the practice of what's called "paving the cow path."<sup>20</sup> A look at a map of Boston reveals a tangled, swerving network of roads, seemingly devoid of forethought and planning—precisely because it *is* largely devoid of forethought and planning, reflecting instead the concretization of human routines.

How roads are planned affects how you live your life in a city. In a place like Boston, you have to know where you are and where you're going—there's no predictable logic you can use to plot your path from, say, Faneuil Hall to Chinatown. Compare this with the experience of getting out of a subway station at 14th Street in Manhattan. Even if you don't know the city, you can use logic to determine that heading in a southerly direction means counting down to 13th Street, 12th Street, and so on.

First principles thinking also matters because it represents a chasm between how technologists approach a problem and how government officials approach a problem. As the stewards of taxpayer money, governments are guided—in theory, at least—by finding the most cost-effective solution that will cause the least amount of disruption in people's lives. Technologists, on the other hand, are all about disruption—so much so that the very term "disruption" has become a cliché in the field. The aim of technologists is to find the *best* solution, not the most inexpensive one that causes the least amount of upheaval. And what better place to explore the very foundation of a problem than where people live and how they get around? In other words, cities.

The problem with technologists increasingly investing energy, time, and money in cities and their infrastructure comes down to two key points: access and the public interest.

The access issue relates to whether what was "public" transportation (for instance) in the past continues to be equally accessible to ev-

everyone under net state supervision. Government, after all, is a servant of “the people.” It’s required by law to serve *all* the people: those who can easily adapt to new services and spaces as well as the most vulnerable among us who cannot. “It’s easy to be good,” Mayor Duarte Eustáquio Júnior, who governs the Brazilian city of Mariana, once told me. “It’s much harder to be fair.”

Technologists may indeed be *thinking* about doing good; fairness, however, is not necessarily the highest item on their priority list. This is not out of malice, but simply because a fairness orientation goes against first principles thinking, which would scrap all assumptions and just build the best possible tech, period, not the perhaps-mediocre-but-hey-it-works-for-everyone tech. Fairness means ensuring that *everyone* has equal access—that the disabled, the disadvantaged, and the infirm have the same access as the able-bodied, the young, and the wealthy.

From this perspective, could we consider the iPhone, for instance, to be “fair”? It did introduce the accessibility feature VoiceOver—a function that lets you double-tap anything on the screen to have it read aloud—in 2009.<sup>21</sup> That’s just two years after the iPhone hit the market, so Apple is apparently doing pretty well at introducing features to make their product accessible to the visually impaired.

But what about to the disadvantaged? iPhones are the most expensive smartphones out there, topping \$1,000 back in 2017.<sup>22</sup> By 2019, a top-of-the-line iPhone XS cost \$1,449,<sup>23</sup> exceeding the average American’s monthly mortgage payment of \$1,030<sup>24</sup> by hundreds of dollars.

Here’s where net states and nation-states sharply diverge: the nation-state is responsible for *all* of its people, not just those who can afford services or don’t need special accommodations. When net states or other private-sector entities begin taking over what used to be public infrastructure, who will ensure that those roads, squares, trains—or entire cities, in the case of Quayside—and other services are fair? Just as we saw in the example of Tesla and Google in Puerto Rico, net states might *choose* to do something to benefit the public, but they’re not *required* to—nor are they are required to be *fair*, as governments are. And this is

where governments handing over public services to net states becomes worrisome.

If the first question is, Who's looking out for public *access*? the next is, Who's looking out for the public *interest*? This is perhaps best illustrated through an example.

Take Waze, for instance, the crowdsourced navigation system acquired by Google. Waze used to rely primarily on data that users input directly, such as instances of traffic jams, accidents, or other obstacles on the roads. Then, in 2014, Waze launched the Connected Citizens program, partnering with 10 locales around the world—including Boston, the states of Florida and Utah, and the New York City Police Department—so that they could include in their app government-owned traffic data, including that from traffic sensors and street cameras.

What exactly does this platform include? Many cities have already begun to adopt smart city technologies with respect to traffic lights. At most recent count, 363 cities across the United States have swapped out traditional traffic lights for modern adaptive traffic control systems (ATCSs).<sup>25</sup>

ATCSs are pretty much what they sound like: traffic systems that adapt the timing of signals based on what they can detect from current traffic conditions.<sup>26</sup> These systems help to reduce traffic jams, which cause substantial problems in cities of all sizes. According to the INRIX Global Traffic Scorecard, in 2019 the average commuter will lose 97 hours just sitting idle in traffic. This costs Americans \$87 billion in lost time—an average of \$1,348 per driver.<sup>27</sup>

Even more important, smart traffic systems save lives. “If you have a smooth traffic flow, that potentially will reduce the number of accidents. Every time you make a stop, there’s a chance of a rear-end collision,” said Aleksandar Stevanovic, director of the Laboratory for Adaptive Traffic Operations and Management at Florida Atlantic University. With roughly 1.7 million incidents of this type in the United States each year, rear-end collisions make up 40 percent of all traffic accidents, killing 1,700 people annually and injuring another half million.<sup>28</sup>

With this context in mind, it's understandable that so many cities are scrambling to implement smart traffic technologies. As with Quayside, the trick is figuring out who controls these technologies and who's in charge of the data they produce.

It seems like it should be citizens. After all, taxpayer money pays for traffic sensors and street cameras. And we as citizens tolerate sensors and street cameras because they provide a public good: in addition to reducing traffic congestion, sensors and street cameras make our streets safer. However, Waze used data from sensors and street cameras to create a feature on its app that serves as a police locator. This is to alert drivers about the presence of police, most likely so they know to slow down to avoid getting speeding tickets. The police locator, however, could also theoretically be used by criminals to pinpoint where cops are stationed throughout the city for the purpose of avoiding the police when committing crimes. This precise complaint was lodged by Charlie Beck of the Los Angeles Police, who wrote in a letter to Waze that the police locator could be “misused by those with criminal intent to endanger police officers and the community.”<sup>29</sup>

This is purportedly what happened when two New York City police officers were gunned down and killed in their patrol car on December 20, 2014. The gunman's phone contained screenshots of Waze's police locator, indicating that he may have used the Waze app to pinpoint the location of the police officers he targeted in the days leading up to his lethal attack.<sup>30</sup>

Clearly, the technologists at Waze did not include the police-tracking feature to facilitate crime. Indeed, Waze's spokesperson reported that the company's relationship with police departments “keep[s] citizens safe, promote[s] faster emergency response and help[s] alleviate traffic congestion.”

Yet this example shows how technology designed with first principles thinking can be manipulated in unexpected and unfortunate ways. It turns out that sometimes there are good reasons—public safety and access for all citizens among them—for assumptions and previously im-

plemented approaches. Waze's programmers were most likely just trying to make the best navigator app they could. The more features they could include, the better the product would be. But coders and software engineers aren't policy experts; they don't necessarily think about the potential impact of their wares on the public in the ways that government officials might. While net states should absolutely continue to innovate ways to make our cities smarter, more connected, and better for citizen-users to live in, governments cannot simply step to the sidelines and watch them do so. They must be integral partners to ensure that innovation doesn't leapfrog over boring yet necessary considerations such as public safety and fair and universal access.

The example above shows public taxpayer dollars being spent on a tech system that may, in fact, have made the public less safe by putting law enforcement in harm's way. This raises the question of whether the people of New York City actually approved of a partnership between Waze and the NYPD. Did they even know about it? It wasn't exactly advertised: in the city's press release announcing the Connected Citizens partnership, Waze was never mentioned, and even Google was mentioned only as one "partner" among many in an announcement on a series of tech partnerships.<sup>31</sup>

While dragging up a vaguely worded press release may seem nitpicky, it underscores a critical point: the people of New York City—*citizens* to the police and *users* to Waze—were taken out of this endeavor's equation. Citizens should have the right to weigh in on how their taxes are spent, and citizen-users should have the right to weigh in on whether they approve of new features in their tech. Just as cities like New York should solicit input from citizens on partnerships that may affect public safety, net states like Google, Waze's parent company, should recognize that the people who use their apps are not just users, but citizen-users whose physical welfare is affected by their technological products and services.

If net states start to recognize citizen-users as such, they may be more likely to invest in adding policy experts to their teams of cod-

ers and designers. In this way, they would be able to meet the comprehensive needs of citizen-users, including public safety, and not just the needs obviously related to their app (say, traffic navigation).

One last risk inherent in the IOT and smart cities is, as with all things digital, their vulnerability to attack. In 2013, Iranian hackers launched a cyberattack on a small dam in Rye Brook, New York, a town 30 miles north of Grand Central Station in midtown Manhattan, successfully accessing its command and control system. A nuclear power plant near Burlington, Kansas, was targeted by Russian hackers in May 2017. Unsurprisingly, dams and nuclear power plants count among the 16 sectors that the US Department of Homeland Security deems “critical infrastructure”: defined as any sector “so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.”<sup>32</sup>

Security agencies rarely report details on such attacks—the Rye Brook dam attack was reported on only three years after the breach—making it difficult to discern how vulnerable the nation’s critical infrastructure really is. But attacks on what are known as SCADA systems—supervisory control and data acquisition systems, which are increasingly used to manage infrastructure—have skyrocketed globally, from 90,000 in 2012 to 675,000 in 2014, a staggering 650 percent increase.<sup>33</sup>

As with most innovations, there’s a tradeoff with the IOT. The more technologically connected our infrastructure, the more we can learn about the human condition: how we live, where we go, what we do, en masse. At the same time, we become more exposed and more vulnerable. The question is whether the tradeoff will be worth it.

THERE ARE SOME REASONS TO TAKE HEART THAT NET STATES SUCH AS Google and Tesla are increasingly investing in, and thus in charge of, future-leaning infrastructure projects. In addition to expanding into cities’ electric grids, as described in chapter 2, Tesla is investing in

transportation projects: the city of Chicago has approved Tesla affiliate Boring Company's proposal to build a high-speed transit system from its O'Hare airport to its downtown area.<sup>34</sup> The reason? Given that technology is their core business, net states may be in a better position than governments to manage high-tech projects.

Often bogged down by politics and bureaucracy, government doesn't have a great track record when it comes to implementing and managing tech projects, especially in the United States. Take Social Security, for example. In 2000, recognizing that a massive backlog of claims had amassed, Congress approved an overhaul of the claims-processing technology used by the Social Security Administration (SSA). By 2007, the SSA had spent upwards of \$381 million trying to integrate its 54 separate information technology (IT) systems, followed by another \$200 million in 2011.<sup>35</sup> Six years after they'd launched the project, "they found out that they really didn't have anything. In fact," commented reporter Bob Charette, "the initial system has consistently been projected to be 24 to 32 months away. So for five years, it was always kind of like Wimpy in Popeye: 'I'll gladly pay you on Tuesday for a hamburger today.'" The rest of the US government doesn't fare much better, and it's no wonder: 70 percent of government IT budget dollars go to maintaining legacy—read "really, really old"—systems.<sup>36</sup>

Again, though, even though net states may be in better positions to successfully pull off large-scale technology infrastructure projects, they are ultimately not legally required to act in the public interest. Net states have shareholders. They have bottom lines. Democratic governments may be delinquent in how they execute their policies, but at least they work to ensure that those policies serve all their people. In the absence of government regulation of technology, especially as it pertains to data sharing, there's no guarantee that net states will choose to protect people's rights as new data sets become available in a suddenly digitized physical environment. While attempts to protect user data exist here and there, we still lack a cohesive guide that countries and net states can follow to protect user data. As data scientist Venkat

Motupalli wrote, “There is a bewildering array of acts, guidance, and agreements across dozens of countries that attempt to address the new size and shareability of citizen data.” Most important, he noted, “While almost everyone agrees that personal data should be protected, there is little consensus as to how and who should be responsible.”<sup>37</sup>

In the absence of consensus, net states are left to take up the responsibility for themselves. And, in the absence of protests from their populations—the citizen-users who use their products and services—they will most likely continue along the path they’ve taken thus far: sharing data with their partners, not only to fuel innovation, but also to maximize profit.

BEFORE WE DELVE INTO THE NEXT PHASE OF FUTURE TECH, IT’S USEFUL to reflect for a moment on how our relationship with technology flipped from active to passive—and how fast that happened. With the IOT, our physical environments—from our smart homes to our neighborhoods, with devices embedded in appliances, roads, traffic lights, and sidewalks—are the active agents, the data collectors. We, the users, are passive; we’re the data creators, the things being observed. The IOT requires no special action from us, just that we go about our business—nothing to see here.

This is a tectonic shift in our relationship with tech. Not two decades ago, our physical environments were dumb, inert. Even our *digital* environments weren’t all that capable. It wasn’t until websites became interactive that we entered a truly dynamic relationship with our technology. Up until then, information flowed along a one-way street, from human to machine. Even with that, we—people—remained in the driver’s seat; we *chose* what information to give our tech.

And we chose carefully—in the early days, at least. We were hesitant, distrustful even. We didn’t even reveal our true names. Indeed, most early websites not only permitted anonymous interaction with their sites; it was the norm.

This was by design, a manifestation of the early web's influence by hacker culture. As web scholar Derek Powazek noted, "Back then, it was normal to have a pseudonym or 'handle' that you went by. Most communication online was hidden behind handles, which reinforced the idea that the internet was not 'real' in the same way real life was. People treated everything online like a game. It was 'cyberspace,' not reality."<sup>38</sup> Our handles both identified and in some ways defined us to others online.

Then came e-commerce, which effectively killed anonymity as common practice. After all, you couldn't use a credit card to order a book on Amazon without giving up your real name. Soon even free websites began requesting "registration"—inviting you to explore their sites for free, so long as you created an account using, at the very least, a name (which could of course be faked) and an email address (which could also be created using a fake name).

For a long while, this seemed like an eminently reasonable tradeoff. After all, websites were entirely free back then—as they remain today, for the most part. While the *devices* that grant access to what's online can involve substantial costs, once you're on your phone or computer, you can peruse the world's knowledge—from maps to media to movies—largely without spending a dime.

Even if you did have to give up some identifying information about yourself in the early years, doing so yielded perks. In 1998, Amazon launched "item-based collaborative filtering"—or, in plain English, the recommendation system.<sup>39</sup> This marked a turning point in how we shop. "Amazon.com has been building a store for every customer," noted Amazon's Brent Smith in a study on its recommendation system. "Each person who comes to Amazon.com sees it differently, because it's individually personalized based on their interests. It's as if you walked into a store and the shelves started rearranging themselves, with what you might want moving to the front, and what you're unlikely to be interested in shuffling further away."

Here's how this translates to a person's actual life. In 1998, e-

commerce accounted for only 0.8 percent of all sales in the United States.<sup>40</sup> This means that nearly the entire population had to go to a physical store if they wanted to buy something. That store looked the same for you and me and everyone else who entered. You had to browse the aisles, maybe ask a salesperson for help, and wait in line to pay; then, eventually, your clothes or books or groceries were bagged and packaged, and off you went.

Enter Amazon. Let's say I go to the site. Because I've bought a few books there in the past, I'm now shown books similar to those purchases. But when *you* go to the site, you see entirely different books, based on the books *you've* bought. With just a few clicks, you go on to buy from the books recommended to you—all without interacting with a single human.

Note: it's not a salesperson who has sized you up and proposed a product to you based on personal judgment and experience.<sup>41</sup> It's an algorithm. And the algorithm probably did a better job of assessing your tastes than that human salesperson. Already by the 2000s, the algorithm could do a better job of recommending the books or movies you liked than even your best friend could. It now knows you better than anyone because it's mirroring you. It does such a good job that Amazon won an Emmy for its personalized recommendation system for video discovery in 2013.<sup>42</sup>

Recommendation systems have become so sophisticated that they can tailor offerings to you from your first visit to a site—what's referred to as a “cold start,” where you've yet to input any information that the recommendation system can draw from.<sup>43</sup> Even in cold start cases, Amazon can draw on “implicit interactions”: the date, time of day, and your geographic location. Based only on these three bits of information, it can then recommend items that others who live in your zip code and browse Amazon at, say, 3:00 a.m. have also purchased.<sup>44</sup>

If you've shared your specific preferences—or, as noted above, just by virtue of the location of your ISP address—recommendation systems customize the web for you whether you want them to or not. We live in a

digital world that is tailored to our likes and tastes. *My* web experience doesn't look like *your* web experience—or anyone else's, for that matter. Based on the fact that I'm researching this book, read sci-fi for fun, and have kids, Amazon offers me titles on the history of Google and Facebook, biographies of Isaac Asimov, and manuals on mindful parenting. It's a combination of products designed for me and me alone.

But this raises the inevitable question of what it means that the web “knows” me—and if it's too late to do anything about it.

The comic W. C. Fields once wrote, “It ain't what they call you, it's what you answer to.” Recommendation systems know us not because of what we *tell* them we want, but because of what we're willing to put money on wanting. In other words, since we buy only things we want or need, recommendation systems call out to us, offering precisely the kinds of products we've given them evidence of wanting and needing. They display products as do salespeople who guide us through a store. The difference is that they take us directly to the wares we do, in fact, really like, even if we may not want to admit to it. While Facebook may permit us to create idealized versions of ourselves on our profiles, recommendation systems know the real us. They mirror our desires. In this way, they are perhaps the most honest reflections of ourselves in the digital world.

There's a lot to be said for recommendation systems. They may help us make wonderful discoveries of new books, movies, and products that we never would have found otherwise. But there's a hidden cost to being so well known. We become less a simple consumer and more a profile of consumer behaviors—a data set that maps our browsing patterns (by how long we spend per product page), purchase temptations (by what we put in our shopping carts and later delete), and commitments (by the products we actually purchase).

If this profile were merely stored in Amazon's database, waiting until our next visit to the website to be launched into action, it would seem a clear-cut victory for consumers: tailored, customized sales support, plain and simple.

But it's not, of course. Amazon and Netflix and YouTube and likely any other website with a recommendation system spell out clearly in their terms of service that your information may be shared with "third parties." Amazon attempts to deflect this in its privacy notice. To the question "Does Amazon.com Share the Information It Receives?" the response reads, "Information about our customers is an important part of our business, and we are not in the business of selling it to others."<sup>45</sup> Great, if that were the whole story. But it's not. The privacy notice then details all the ways in which they *do* share your information with others, including "Marketplace Sellers," or "businesses [that] operate stores at Amazon.com or sell offerings to you at Amazon.com." This would account for a whopping 52 percent of all sales on Amazon.<sup>46</sup>

Amazon also shares your personal data with third parties for the purposes of "fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service." In short, just about every step of the transaction process at Amazon involves third parties. So, while Amazon may not "sell" your data, it certainly does share it with numerous third parties.

This matters because we no longer transmit data only when we're aware that we're online. Our data from conscious actions, such as making purchases on Amazon, as well as the data that streams almost constantly in the background, gets gobbled up by various third-party data brokers to create ever more detailed profiles on us.

AMAZON HAS SINCE EVOLVED. IT MADE ITS MARK BY "KNOWING" US: identifying our wants and needs and providing recommendations for other things we might want based on those wants and needs. But it wants to know us even better—not just our preferences, but our physical profiles as well. With its new recognition software, Amazon is now

wading into the IOT.

Foundationally, recognition software isn't so different from recommendation systems. Both know you—an individual user—in a way. Both can identify you based on various attributes: your likes and preferences, for recommendation agents; your physical characteristics, for recognition software.

Yet, while the foundations are similar, the aims are very different. Amazon's recommendation systems identify you for the purpose of showing you stuff you like. Rekognition, as Amazon's facial recognition system is called, identifies you for the purpose of pinpointing you for law enforcement, with the aim of getting you translated into a profile in a police database.

The ultimate aim, of course, is public safety. If law enforcement officers can pick a known criminal out of a crowd on a busy street, they can move to protect other citizens from that criminal. But questions have emerged regarding how the system works and who handles the data collected.

Rekognition is already being tested in real life—police departments scattered across the country use the system, though few advertise that fact. Amazon boasted in a 2017 blog post that Rekognition can detect “up to 100 faces in challenging crowded photos”<sup>47</sup> and proudly lists the Washington County, Oregon, Sheriff's Department on its Rekognition website as a satisfied customer. The department reciprocated, testifying on the Amazon Web Services (AWS) website that they “were able to index more than 300,000 photo records within 1–2 days, and the identification time of suspects went from 2–3 days down to minutes.”<sup>48</sup>

While the US surveillance system is far less developed than that of countries like the United Kingdom, which has over 6 million closed-circuit television (CCTV) cameras,<sup>49</sup> or China, with 570 million cameras,<sup>50</sup> we fundamentally diverge with those camera-heavy countries with respect to owner and operator. In the UK, their CCTV network is operated by the government of the UK; in China, it's the government of China. Yet it is *not* US law enforcement agencies that developed and

deploy surveillance technology in this country; it's Amazon. And it is *not* US law enforcement agencies that wholly own the data they input into their surveillance technology: it's Amazon.<sup>51</sup> Recall, law enforcement agencies, being an arm of the nation-state government, are legally prohibited from monetizing, making public, or sharing personally identifiable information (PII) with anyone.

But Amazon is a private corporation. No laws yet regulate what it can do with its data. As of this writing, it and any other net state that cares to get into the surveillance game can share with as many third parties as they see fit.

Doing so has not been without controversy. The American Civil Liberties Union (ACLU) publicly criticized Amazon for marketing directly to police departments.<sup>52</sup> Independent privacy scholars have also expressed concern: "The idea that a massive and highly resourced company like Amazon has moved decisively into this space"—meaning, directly marketing to law enforcement entities—"could mark a sea change for this technology," said Alvaro Bedoya, executive director of the Center on Privacy and Technology at Georgetown University Law Center.<sup>53</sup>

In some ways, the fact that net states are moving into law enforcement support is not exactly shocking, or even all that new. Security agencies from the NSA down to local sheriff departments have been using computer systems to track and monitor criminal activity for decades. In a way, implementing facial recognition software might be seen as a natural evolution to what beat cops have been doing for years: picking out faces from a crowd for the purpose of getting criminals off the street.

The problem is, law enforcement doesn't exactly have a squeaky-clean record in terms of *who* it picks out of a crowd. When Congress heard about Rekognition's use in law enforcement offices, several members of Congress, led by Rep. Jimmy Gomez (D-CA) and Rep. John Lewis (D-GA), as well as the Congressional Black Caucus, sent letters of concern to Amazon CEO Jeff Bezos, citing studies showing that facial recognition software consistently misidentifies minorities—specifically,

persons of color and especially female persons of color.<sup>54</sup> The software misidentified white men 0.6 percent of the time but misidentified women of color 35 percent of the time. According to an MIT study of the technology, this was due to the fact that the data set training the program was 77 percent male and 83 percent white.<sup>55</sup>

“Surveillance of perfectly legitimate and constitutionally protected activity will only further erode the public’s trust in law enforcement,” Chairman Cedric L. Richmond (D-LA) wrote in his letter to Bezos. “We urge you to be thoughtful, deliberate, and assiduous as development of this technology advances.”

This is the key question: Are these technological advances being thought through—and, if so, how and by whom? Or are advances simply made because they’re the next logical step in tech’s evolution?

Scott Carpenter, Google Jigsaw’s managing director, isn’t optimistic. “A lot of companies, they’re just trying to get off the mat and into the game,” he said. Right now, the implications of how their tech will be used in the future is less a consideration than figuring out how to get their tech used at all. Tech users—you and I and all of us—are responsible to hold our net states to account for the ways that their new technology is being implemented.

But we can’t do that if their use is secret. This is the crux of the ACLU’s argument against law enforcement’s use of Rekognition. As the *Washington Post* reported, “Not even the FBI is using its facial recognition software to track people in real time.”<sup>56</sup> Privacy scholar Alvaro Bedoya was quoted in that article as saying that the ACLU’s findings are the “clearest example yet that these dragnet, real-time face recognition systems are real.”

AMAZON KNOWS MUCH ABOUT US, AS WE’VE SEEN. THROUGH OUR browsing patterns, it knows what products tempt us. Through our purchase history, it knows what products triumph over us. Through these, it can infer our drives and impulses and create a profile of our consump-

tion behavior—a mirror of who we are as people. With Rekognition, it will be able to assign a face to the behavior. With Amazon's home assistant, the Echo, it can also assign a voice to the face and the behavior. The question then becomes: If tech can know what we do, what we want, what we sound like, and what we look like, what's left? Are we truly and fully known by our net states? And, if so, what happens with that knowledge?

It would be naive to think that net states won't make use of this knowledge for some purpose. Evgeny Morozov, who has taken on the mantle of resident technology distruster, recently dubbed this practice “data extractivism”; he argues that its purpose is to train artificial intelligence systems.<sup>57</sup> “Once built,” Morozov argues, “this AI capacity can be lucratively rented out to governments and companies.”

With the IOT and smart cities, citizen-users will feed the net states with databases that profile us. Will we be aware that it's happening? And, if so, will we care?

As it turns out, people report worrying about what happens to their data, but they're not willing to give up their tech to protect it. “The trust train has left the station,” as one professor reported to the Pew Research Center for Internet and Technology in a survey on technology and trust.<sup>58</sup> A software engineer wrote in the same survey, “People's trust will have zero correlation with reality. It is not appropriate to expect their feelings of trust to correlate with actual technological details.”

Trust in technology may indeed be an issue of the past. It's certainly not the driving factor people rely on when they decide whether to use technology. Convenience, connection with people we care about, and plain old curiosity are much better indicators of whether we'll sign various terms of service and give away our data to parties unknown.

In this way, Amazon knew us best from the very beginning: we don't look to tech for trust, we look to *other people* for trust. The customer reviews on Amazon—the first of any site on the web—got it right. We want to hear from other people what they think about the world. We want to get in on the experience they describe, whether it be a book or

film or product we're told they just can't live without. And, in this way, we simply want to be connected with others; to be part of the conversation, even if it's just as an anonymous, passive observer peeking in on an online comment. For by reading others' thoughts, we are less alone with our own thoughts. And perhaps we feel just a little less alone.

We may not trust tech, but somewhere deep down, we still trust people—even strangers online. Technology is simply the conduit that gives us access to others, especially like-minded others who love the same books we love, the same movies and gadgets. For all the ways that tech isolates us, it also creates avenues for connection to a quasi-experience of kinship—ways to find others like us, who like what we like and want what we want. It may not be as satisfying as a friendship with a person we exchange words with, but maybe it's better than no connection at all.

The IOT won't connect us to other people—yet. It connects tech to other tech. But the data collected by IOT devices will be applied to some purpose at some point. And, if history provides any indication, increased connection to others like us is a fair bet for future applications. For all our solitary endeavors, we are social creatures. And we love finding others who love what we love. Net states would be wise to capitalize, and likely already are capitalizing, on that for their next generation of products and services: providing yet more ways for us to find a feeling of serendipity—even if we know deep down it's just an algorithmically generated facsimile.



## SEVEN



# THE MIND, IMMERSED

This chapter moves from our habits to our head, exploring what happens to our brain, for good and ill, when engaging with net state technology. It describes how immersive technologies, starting with our most closely held technology—the smartphone—both facilitate learning and interfere with cognition. It also examines what we stand to gain from new forms of immersive tech and asks how our desire for mediated reality that’s especially designed for us as individuals might be fulfilled by these new technologies (and what that fragmenting of experiences might mean for us as a people).

The modern person drives a lot. And much of the technology installed in our cars has made transportation radically safer than in the past. For instance, the National Highway Traffic Safety Administration estimated in 2017 that airbags alone had saved 50,457 lives in the US since they were first introduced in 1987—the number of people it would take to fill a major-league baseball stadium.<sup>1</sup>

Yet some of the technology we *use* in our cars may endanger us and the people around us even more dramatically. This section explores how.

On an average day in 2018, American car-owners spent 55 minutes apiece behind the wheel, taking, as a group, approximately 1.1 billion car trips.<sup>2</sup> That's 1.1 billion chances, every day, that someone—managing a complicated piece of machinery hurtling through space at high velocity with thousands of other vehicles doing the same in the face of countless potential distractions—could crash.

But, for the most part, people don't. Despite distractions from the weather, the road, the radio, other drivers, passengers, food, and beverages, we manage—by and large—not to drive our cars off the road in a fiery blaze.

This holds true even when we space out—and apparently we do that a lot. According to a 2016 report published by the National Institutes of Health (NIH), every single respondent in the study admitted to “mind wandering” every time he or she drove.<sup>3</sup> “Mind wandering” behind the wheel of a car sounds like a recipe for disaster. But statistics suggest that people overwhelmingly manage to stay on the road, despite being checked out at least part of the time.

Consider the numbers: in 2018, nine of every 1.1 billion car trips ended in a fatal car crash due to distracted driving.<sup>4</sup> That sounds like a lot, and even one fatal crash is, of course, too many. But let's change the perspective for a second and consider this statistic another way: out of the 1.1 billion car trips taken every day, fewer than 0.000001 percent of them resulted in a fatality related to distracted driving. Statistically speaking, that's a bizarrely small percentage.

To understand what really happens in our brain when we're operating a car, a team of research scientists at the University of Texas decided to study drivers during episodes of various types of distraction. In a study published in *Nature* in 2016, they found that drivers were surprisingly capable of staying on the road, not only in the presence of garden-variety mind wandering, but even when experiencing emotionally distressing thoughts and cognitively demanding tasks.<sup>5</sup>

What they found is that even when we don't pay active attention, some part of our brain keeps watch. As Ioannis Pavlidis, who led the

study, remarked, “The driver’s mind can wander and his or her feelings may boil, but a sixth sense keeps a person safe, at least in terms of veering off course.”<sup>6</sup>

This “sixth sense” refers to the part of the brain—the anterior cingulate cortex, or ACC—that automatically intervenes when it detects conflict from cognitive, emotional, or sensorimotor stressors. In other words, we can space out or think angry, sad, disturbing, or distressing thoughts and still not crash because there’s a part of our brain standing guard. The brain’s ACC minds the sensory-information shop, so to speak, and ensures that whatever we smell or taste or hear or see or feel that is somehow not right triggers a response.

There is, however, one exception that prevents this sixth sense from working—one activity that fails to trigger the ACC’s intervention response.

I’m sure this won’t surprise you: it’s texting.

Based on the findings in Pavlidis’s study, the only time the ACC failed was when people engaged with their phones. The subjects’ neurological watchdog simply went offline. “The moral of the story,” Pavlidis explained, “is that humans have their own auto systems that work wonders . . . until they break.” Ultimately, what is causing the systems to break is tech.

This holds for anytime we’re using our tech. Take walking. Emergency room visits for pedestrian injuries increased a sobering 500 percent from 2005 and 2010.<sup>7</sup> And the most tech-obsessed demographic is also, depressingly, the hardest hit: in 2016, out of almost 6,000 pedestrian fatalities by cars, 61 percent were 15 to 19 years old, with most deaths due to what the National Safety Council described as “distracted walking”—that is, walking while immersed in one’s tech.<sup>8</sup>

We’ll delve later into what it is *about* tech that causes the break in our ability to save ourselves. Suffice it to say here that something about using tech wreaks havoc on our neurological protection system; tech is too immersive, too distracting—too *something*—to let our brain step in and save us from the consequences of inattention. In other words, some-

thing about tech draws us in—and not just our active mind, but our subconscious—even to the point where it can put us in danger.

“TECHNOLOGY MAKES US SMARTER.”

“Technology makes us stupid.”

“Technology is an extension of our brain.”

“Technology impedes our ability to think.”

And so goes the debate about the effects of technology on our thinking. Rather than hash out every aspect of the tech/brain debate, let's focus on the most personal aspects of our relationship with net states: how our technology use impacts our ability to learn, focus, and function. Let's look at the first of these abilities next. We'll circle around to the latter two later in the chapter, when considering internet negatives.

Of that bunch—learning, focusing, and functioning—learning is the given for positive impact. If our capacity to learn is tied in part to having access to materials from which to learn, then technology provides a slam-dunk win for the human race. Technology provides more *opportunities* to learn—not necessarily to focus or recall, but to find information that can teach us stuff. As technology has evolved into smaller, more personalized devices, we can take advantage of opportunities to learn faster and more easily than ever before. Consider that just two decades ago, if you didn't know the capital of Mongolia or how to calculate standard deviation, you'd have to look it up in a book in your home, if you happened to have an encyclopedia or a statistics textbook, or physically go to a library or bookstore. Now, thanks to Google and Bing and other search engines, the answers are literally seconds away. (That would be Ulaanbaatar and, well, you can look up how to calculate standard deviation yourself.)

Microsoft may have brought computing to the masses, but it was Apple that made computing an individualized experience. From the iMac to the iPod to the iPhone, Apple made computing increasingly personal throughout its product evolution. As noted previously, the key is in the

marketing label “i”: tech products for you and you alone. For decades, Apple has promoted computing as a relationship between human and machine, and a very intimate one, at that. True, encouraging each individual to buy their own Apple computer or phone rather than sharing one with their family means that Apple sells more Apple products. But there’s more to it than that.

Throughout the history of Apple’s computer products, they have been the drivers behind making tech smaller and more portable. Back in the early 1990s, it was eminently reasonable that each household would have only one computer: desktops were big; you needed a desk to house the tower—the computer itself—plus the monitor, mouse, keyboard, and modem—all of which were separate, space-consuming devices. Apple led the way toward shrinking tech products, starting with its earliest desktops and leaping into the modern age in 1999 with the unveiling of the iMac—available in five candy-pretty colors.<sup>9</sup>

Despite the size—it was still a hefty machine, weighing in at 40 pounds—it begged for personalization: one’s teenage daughter might opt for tangerine, while the grown-ups in the house might choose the slightly more muted blueberry.<sup>10</sup> Then with the iPod music player in 2001, Apple’s offerings graduated from customizable machines to customizable music collections. With the iPod, users could not only upload just the music *they* liked, but make multiple playlists. With this move, users liberated themselves from the studio album format and began creating their own versions of albums with as many artists as they wanted.

Finally, the iPhone arrived in 2007, taking Apple’s personalization/shrinkage quest to a whole new level. In a single, pocketable device, web browsing and picture-taking and texting and game-playing were suddenly available to you and you alone, anywhere you happened to be. Users were now liberated from the desk and from the house. With the iPhone, the internet left the building.

Here’s how the iPhone relates to our intelligence—or, specifically, our learning.

According to what’s known as “the Flynn effect,” IQs—intelligence

quotients—have been steadily rising over the past hundred years, gaining approximately 30 points worldwide across that century.<sup>11</sup> This means that the average person in 2012 (when the study was conducted) is smarter than 95 percent of the population from 1900.

While several factors likely contributed to this effect, including better nutrition and medicine, the global revolution in schooling remains the most influential contributor. In 1900, for instance, only 6 percent of Americans had a high school diploma.<sup>12</sup> Compare this with 88 percent of Americans in 2015.<sup>13</sup> Higher education was even more elusive a century ago. In 1900, only 3 percent of the population had finished college. By 2014, more than 40 percent of Americans had college degrees.<sup>14</sup> A meta-analysis of studies suggests a direct correlation between how many years one attends school and his or her IQ score, with a global composite average of an additional 1.9 IQ points gained for every year of schooling.<sup>15</sup> The general takeaway here is that, on the whole, greater education yields a slight increase in cognitive abilities.

Learning is certainly associated with formal schooling, but teaching oneself counts, too. And thanks to the internet, opportunities for self-education have exploded. According to a study by the Pew Research Center for Internet and Technology, Americans with technology assets that include a smartphone *and* a broadband connection are much more likely to engage in personal learning than those without tech.<sup>16</sup> And we don't feel forced to learn; we dig it—72 percent of respondents report enjoying having access to so much information online, with only 26 percent reporting feeling “overloaded.”<sup>17</sup>

Perhaps in some ways, the reason most of us don't feel overloaded is simply that we've adapted to our current reality. As James R. Flynn, the scientist behind the rising IQs study and author of the book *Are We Getting Smarter?*, noted in an interview, our increased IQs and global commitment to educating our youth don't mean we're somehow better than our counterparts of a century ago; we've simply adapted to a more complex information environment. We *needed* to become smarter, in other words, to be able to manage more complex information. Indeed,

it's not that the entire year-1900 population wrestled through a daily struggle to survive, dragged down by their "low" IQ scores. For 1900, their scores weren't low at all. They were just era-appropriate—exactly the kind of IQ necessary to cope with *their* information environment. The world that people encountered simply wasn't as complicated back then; 30 fewer IQ points was no hardship, it was the norm. So, while we can view the global elevation of IQ points as a sign that we are becoming smarter as a people, we didn't really have a choice in the matter—improved cognitive abilities were, perhaps, just a natural adaptation for us to survive in the complex landscape that defines our time.<sup>18</sup>

This landscape is both fueled and shaped by technology. As noted, the internet makes self-education easier than ever. Indeed, the tech *industry* itself is the paragon of self-teaching: 69 percent of coders report being self-taught, as opposed to having learned their skills in a classroom.<sup>19</sup> Even beyond coders, regular people learn things online fairly frequently: 59 percent of Americans use search engines on a daily basis, which equates to roughly 191,750,000 people searching for information daily, totaling around 321,000,000 queries a day.<sup>20</sup>

Clearly, not all queries are about substantive or educational topics. The five most popular search terms in 2017 were "Hurricane Irma," "Matt Lauer," "Tom Petty," "the Super Bowl," and "the Las Vegas shooting."<sup>21</sup> While two of the five concern socially impactful events—the hurricane and the mass shooting in Las Vegas—the others appear to be more focused on entertainment and scandal-of-the-moment curiosity.

But the broader point is actually not *what* people search for; it's *that* they're searching, period. People are curious, and tech provides them the means to satisfy that curiosity. Whether they're inquiring about how to make slime or solar eclipse glasses (those would be the top two "how-to" searches in 2017), or about national tragedies like the largest domestic-terrorist mass shooting in the history of the United States, almost doesn't matter.<sup>22</sup> What matters is that, thanks to tech, people have the power to find things out. And, given the high number of searches that come from mobile devices, we're often finding out things from our

tech the very moment we wish to know them.<sup>23</sup>

Curiosity matters. It's one indicator of cognition—different from IQ, but important in its own right. In fact, in these increasingly complex times, some researchers have suggested that in addition to our IQ, we should take stock of our EQ, our emotional intelligence quotient (or how good we are at recognizing the emotions of ourselves and others), and our CQ, or curiosity quotient (how hungry our mind is to find things out).<sup>24</sup> The reason our curiosity quotient matters so much is that people who are more curious tend to be more comfortable with ambiguity.<sup>25</sup> And comfort with ambiguity is an indicator of tolerance.<sup>26</sup> Tolerating ambiguity—the unknown or the unresolved—is difficult, but it's also really good for us: people who can tolerate unknowns for sustained periods have been shown to be more innovative, more optimistic, less vulnerable to depression, and more comfortable with taking risks.<sup>27</sup>

Clearly, there are downsides to checking our phone 80 times a day on average.<sup>28</sup> It's highly likely that at least some of these checks are compulsive, almost unthinking. We've already established that phone-checking can be a ruse to avoid interacting with people nearby, at least some of the time. But it's also an indicator that we're curious—to learn new things, for new stimulation, for updated information. Regardless of the subject of our curiosity, just being curious is cause (albeit small) to celebrate.

NO ONE IN THE UNITED STATES IS FORCED TO CREATE A SOCIAL MEDIA account, to buy or sell anything online, or even to maintain a digital footprint of any kind. But almost three decades after the advent of the World Wide Web, is it really possible to be a fully functioning citizen without some sort of digital presence? What would digital invisibility cost you?

To answer this requires first understanding the current context. Americans are lucky, digitally speaking. As I'm writing, 90 percent of us have internet access, and that's *high-speed* access for 68 percent of

us.<sup>29</sup> We take advantage of that access too: 90 percent of Americans use the internet on a regular basis.<sup>30</sup>

Which means, of course, that 10 percent of Americans don't. The reasons *for* being online are fairly well understood by now—fast and convenient access to information, services, shopping, social interaction (of a sort), and so on. With all these benefits, several questions arise: Why would anyone stay away? And, in our increasingly digital economy, how would they manage? Finally, is there really any downside to staying offline?

For all the free information online, accessing the internet isn't actually all that cheap. Computers and smartphones cost money—even a cheap laptop runs around \$300, and the going rate on smartphones is \$400 to \$500. Data plans or broadband connections will also cost you: somewhere in the neighborhood of \$75 to \$125 a month for either one. Add this up over the course of a year and you're spending \$1,500 or more just to go online.

But money's not actually the issue. Of the 10 percent of offline Americans, only 19 percent cited lack of money as the prohibitive reason. Over a third reported that they simply weren't interested in the internet or didn't think it was relevant to their lives. Age, income, and educational attainment were all factors associated with being offline—those over 65, those earning less than \$30,000 a year, and those with less than a high school diploma were the most likely groups to stay offline.

These all seem predictable. For example, 47 percent of the group who are offline are over the age of 50, with decreased use more prevalent the older the person. But what's more surprising is the cohort of younger, wealthier, and more educated people who aren't online. *This* group isn't keeping offline because they can't afford internet access or don't understand it. They simply choose not to use it—or don't permit their children to use it.

Chief among this group are the net state developers: in 2018, Silicon Valley parents were among the most likely cohort to keep their children from using the very same technology they created. This group, through

the years, has included Apple's late Steve Jobs, Microsoft's Bill Gates, *WIRED*'s Chris Anderson, and Twitter's Evan Williams, all of whom practiced what's called "low-tech" or "no-tech" parenting.<sup>31</sup>

The rationale behind low-tech parenting is fairly sobering. Tech, in the view of many (including a number of its creators), can do bad things to kids. As Napster founder and former Facebook president Sean Parker put it, "I don't know if I really understood . . . the unintended consequences of a network when it grows to a billion or 2 billion people. . . . It literally changes your relationship with society, with each other. . . . It probably interferes with productivity in weird ways. God only knows what it's doing to our children's brains."<sup>32</sup>

While low-income families struggle to ensure that their children don't miss out on the chance to be "digital natives," the trend among the wealthiest and most tech-savvy among Americans is to keep their children *away* from digital devices for as long as they can. Former Facebook executive Chamath Palihapitiya made headlines when he said publicly that he felt "tremendous guilt" for what he'd helped to create.<sup>33</sup> "The short-term, dopamine-driven feedback loops that we have created are destroying how society works," he said. And he doesn't let himself off the hook for it. "In the back, deep, deep recesses of our mind, we kind of knew something bad could happen."

Keeping children away from social media sites like Facebook or limiting time spent on online games is one thing. There's plenty of research that now supports the notion that excessive use of social media leads to negative health effects, especially among the young, such as anxiety and depression.<sup>34</sup>

But there remains an unexplored question: Beyond parents who choose to keep their children offline, what about adults who can afford internet access and are educated enough to navigate the web, but still choose themselves to remain offline? Why might *they* do it? And more important, what does it cost them, if anything?

One of the first reasons to stay offline is to avoid a digital footprint, a publicly accessible online profile. Strangers can get a pretty detailed

impression of us from reading about us online—and many people aren't comfortable with that.

Even if we don't admit it, most of us have Googled ourselves at some point, if only to ensure that nothing damning or inaccurate comes up in search results. It's time well spent. Employment recruiters attest that one of the first things they do when assessing candidates is to look at their digital footprint. And not having one can be just as problematic as having a negative one. It can signal the absence of tech smarts, as one recruiter reflected: "In the new Millennia, lack of technical skills makes you an employment pariah."<sup>35</sup> Simply put, in our computer-dominated work world, most positions require some degree of technical know-how. The total absence of an online persona may look more suspicious than even a slightly embarrassing one. That's a significant cost to avoiding the internet.

Another reason some adults choose to remain offline is the threat of reduced focus. While we *can* learn just about anything using the tech at our fingertips, tech is killing our concentration, a necessary precondition of learning.

Problem number one, focus-wise, is our technological attention-grabbers. Thanks to haptics—the physical buzzes and tics our phones give off when we get new messages, new calls, new texts, and new alerts—we're physically nudged by our phones, gently yet unfailingly, on a fairly regular basis. This effectively shatters our ability to focus. Tech may make it possible to learn whatever we want, but whether we can pay attention long enough to *process* what we've learned is a different matter entirely.

Most of us have apps on our smartphones, and most of those apps send us alerts. Getting a single notification on our phones may not seem like a big deal. As it turns out, though, we're not the best judge of what constitutes a distraction.

In a recent study, participants were asked how often they got push notifications on their phones. They reported that they got around 20 a day. That's not nothing, but it's a seemingly manageable amount, aver-

aging about 1.2 notifications per waking hour, spread out over 16 hours (assuming most people sleep eight hours). In reality, however, these participants actually received an average of 63 push notifications per day—more like four per waking hour. What's more, participants in the study didn't just *get* the alerts; they usually took the time to unlock their phones and view the notifications within minutes of receipt.<sup>36</sup>

That push notifications might negatively impact the brain isn't hard to imagine. In an NIH study on the specific brain waves associated with concentration and cognition, researchers found that push notifications resulted in impaired cognition in the period immediately following receipt of the notification.<sup>37</sup> What's more, the subset of participants who were deemed at risk for overusing their smartphones also exhibited a diminished ability to complete tasks after receiving notifications. In other words, just getting notifications hindered people's ability to focus. For some people, it hindered their ability to do things as well—in other words, hindered functioning.

Even when we're not getting alerts, our bodies have become conditioned to think we are. In a 2012 study reported in the journal *Computers in Human Behavior*, 90 percent of respondents reported feeling “phantom vibrations”—the eerie sense that their phone was buzzing, even when no alert had come through. And this was fairly frequent: at least once every two weeks.<sup>38</sup>

To track the ill effects of our forever-on technology, a group of former net state engineers who founded the Center for Humane Technology (CHT) created what they called the “Ledger of Harms,” a roster of studies into just how damaging our tech can be to our attention.<sup>39</sup> “This Ledger collects those negative impacts of social media and mobile tech that do not show up on the balance sheets of companies, but on the balance sheet of society,” the website says. That tech creators themselves—the founders of the CHT come from Facebook, Google, and other major net states—have mounted a campaign *against* their own products is a powerful indicator that the current quantity of time we spend with our tech is likely far from benign.

But let's break down what the evidence really means. As we just read, our phone physically prods us 63 times a day, or once every 15 minutes, with a sound or vibration that temporarily annihilates our focus and messes with our ability to function—to do the thing we were doing before we got the notification. Worse yet, checking our phone because we got a notification is just a subset of the overall number of times we check it: that would be an average of 80 times a day, or once every 12 minutes.<sup>40</sup>

There are a number of obvious problems with this intermittent activity. Our train of thought is routinely derailed. Our ability to be present in the moment with the humans standing physically in front of us is greatly diminished. Our neck gets cramped from craning over our phone for long periods. But what's really interesting about this isn't how tech affects our attention, our cognition, or even our ability to function. What's truly intriguing about all of this is the possibility that we're seeing a new kind of information environment that demands its own form of adaptation—a new kind of survival mechanism. It's called the “adaptability quotient.”<sup>41</sup>

Imagine this scenario. You're at work. Your phone buzzes. You check it; then you go back to the email you were in the middle of writing.

Three things have to happen here. First, you have to break away from a train of thought. Second, you have to engage in a new thought process to deal with whatever the notification was about. And third, you have to gather the thoughts that got scattered about when the notification distracted you. If you have a high adaptability quotient, you may be able to train yourself *not* to lose your train of thought, but rather to hold it aside, in a suspension of sorts, so it's still there when you come back to it.

Before we look in more detail at what the adaptability quotient is, let's consider what it is *not*. It may sound a bit like multitasking, but there are key distinctions. First, no one can actually perform multiple tasks at the same time. What we think of as multitasking is actually performing tasks in batches and quickly switching between them.<sup>42</sup> As

it turns out, doing so comes at a cognitive cost. We're ultimately less productive and even less smart: our brains operate at a lower intellectual capacity—our IQ literally drops downward about 10 points—when multitasking. This is because we experience what's called “attention residue,” a sort of mental jetlag that ties us to whatever we were just paying attention to. And it lingers, especially when we've switched to a new task without first completing the previous one.<sup>43</sup>

Attention residue isn't just annoying; it gums up our mental works, stripping us of the ability to cleanly switch cognitive gears. In other words, task-switching before we've finished what we were working on hurts us in multiple ways. First, our original task is left incomplete. Second, we have less brainpower to focus on our new task, making us approach it a little less effectively than if we had just finished the first thing we were doing.

We know from the earlier example about distracted driving that tech shuts down the brain's sensory information monitor, the ACC, whose job it is to detect conflict from cognitive, emotional, or sensorimotor stressors, ensuring that even if we're sort of spacey, we notice when something dangerous comes our way. With the ACC shut down, when something dangerous *does* come our way, we may not notice until it's too late.

Now, consider the number of distractions we get per day via tech: again, 63 notifications. We don't know when we'll get them, but we might anticipate that they're coming. The anticipation alone takes a toll on our cognition. A study in the UK showed that just knowing an unread email was waiting in one's inbox made workers less cognitively capable and resulted in an average loss of 10 to 15 IQ points.<sup>44</sup> As we saw earlier in this chapter, research predicts a 1.9-point increase in IQ for every year of schooling. Turning that finding on its head, we could conclude, based on the IQ loss found in the UK study, that just by virtue of knowing you have an unread email waiting in your inbox, you lose 7.5 years of school, going from being a college graduate to a freshman in high school.

This all points to a big problem. The fact that mere *anticipation* of unread messages obliterates our cognition, and that we anticipate that

we're going to get alerts on our phone every 15 minutes, seems to suggest we are, as a people, probably a bit dumber than we would be without our phones.

Today's constant notification environment is quite new. It started with the pager, a pocket-size device popular in the early 1990s that would alert you to call someone. It may be difficult to imagine more than two decades into the internet era, but pre-pager, once you left your home or office, you were simply unreachable. Unreachable—or free, depending on how you looked at it. Pagers changed all that. You could be pinged (or “beeped”; the other popular moniker for the device was a “beeper”) when someone was trying to reach you, no matter where you were.

Pagers had their moment. Back in 1994, when Motorola dominated the market, more than 61 million people clipped the little things to their belts or tucked them into their pockets.<sup>45</sup> Though physically insubstantial, they changed everything. They were the first mass-produced, reach-me-everywhere device and the first mass distract-me-anywhere device.

In the 20 years since the pager's heyday, technology has only become more immersive—first with cell phones, then with smartphones. Thirty years ago, pre-pager, we had to make a choice to connect with individuals who were not in our geographic vicinity—we had to physically go to them, or go to our home or office or a payphone to call them. Now we've lost the element of choice; we're on the receiving end of alerts telling us that other people want to connect with us—people we know, who have our number and send us texts or emails—and also telling us that certain apps want our attention: weather apps warning of incoming storms, game apps inviting us to pick up where we left off, news apps with “breaking” headlines, social media notifications that someone has flagged us in a tweet or a post. We're in an era of relentless incoming attention-grabbing.

Imagine the IRL equivalent: someone tapping you on the shoulder, no matter where you were or what you were doing, 63 times a day. The difference, of course, is that you can choose to ignore your tech-fueled

shoulder-tapping. Yet, as the studies cited above show, simply getting the notification (even absent reading it) is enough to disrupt your focus. That's because the act of choosing to ignore a notification means first cognitively registering that you got it—all of which temporarily takes you out of the moment, away from doing whatever it is you were doing.

To survive this new threat to our mental functioning, we need to get smarter, but in a new way. We need to be able to adapt, quickly and frequently, to preserve our brainpower. We need an adaptability mechanism that can manage both the *possibility* of distraction and the *actual* distraction from the technology we carry and wear.

Which brings us, at long last, back to the adaptability quotient. Harvard psychologist Robert Kegan argues in his book *Immunity to Change* that to stay relevant and competitive in our distraction-fueled environment, we need to get comfortable with making complicated, complex decisions regularly—so comfortable that we become, in his words, immune to even frequent change.<sup>46</sup> In other words, to survive this era, we need not just intelligence, emotional intelligence, and curiosity, but adaptability as well.

Training ourselves to become more adaptable, all while coping with distraction and the related diminished brainpower, is exhausting. It's no surprise, then, that distractions that create a sense of escape, like television, are as popular as ever. The good news is that there's a silver lining for our brains in our quest to escape our exhausting information environment. Thankfully, it turns out that certain kinds of TV may be just a little bit good for you, albeit in a sneaky way.

To figure out how, we can take a lesson from a high school chemistry teacher who transformed himself into New Mexico's crystal meth king.

Walter White's dying. His wife's pregnant. His teenage son has cerebral palsy. He's so broke that in addition to his job as a high school chemistry teacher, he works a second job at the local car wash. To leave his family something they can use to build a better life after his death, Walter comes to the less-than-obvious conclusion that he should use his chemistry know-how to make crystal meth.

This is the premise behind the Emmy Award–winning show *Breaking Bad*, which aired from 2008 to 2013. It’s one example of a new genre of show that exhibits what academics call “narrative complexity.” Shows with deep narrative complexity—*The Sopranos*, *The Wire*, and *Game of Thrones*, to name a few—use a “historically distinct set of norms of narrational construction and comprehension” that distinguish them from procedural shows like standard sitcoms, cop dramas, or reality shows.<sup>47</sup> They’re what they sound like: complex. They’re not just stories; they’re fictional worlds with massive casts of characters. It is precisely because of their complexity that they’re somewhat good for our brains.

Infusing our entertainment with complex narratives is important because it may very well counterbalance, to some small extent, the cognitive damage done by tech in other ways. To be clear, this is not to suggest that we should seek out *more* screen time or that doing so would be somehow good for us. Rather, it’s a way of seeing one form of screen time we already escape to—TV—from a new perspective.

Ironically, it’s the same tech that distracts us that’s responsible for enabling this new genre of narratively complex shows. Thanks to the proliferation of tech platforms producing television shows—as when Amazon and Netflix entered the market—there was suddenly an appetite for content, opening up space for more shows that experiment with increasingly complex narrative structures.

And narrative complexity does do good things for our brain. It activates areas of the prefrontal cortex associated with episodic memory retrieval, thus enhancing overall memory retrieval abilities.<sup>48</sup> The more complex the characters in the story, the better: character-driven stories stimulate production of oxytocin, the hormone we feel when we experience love.<sup>49</sup> Narratives of all kinds also activate multiple areas of our brain—the language-processing areas, of course, but also, somewhat surprisingly, any area associated with the activity happening in the story.<sup>50</sup> This means watching a story about a person running through a forest activates the area of your brain that deals with your fight-or-flight response, simply because you can imagine running away from

someone.<sup>51</sup>

The real reason this matters is that we continue to spend a lot of time with narratives. We're still watching a lot of TV, upwards of four hours a day.<sup>52</sup> Interestingly, the younger generation—18- to 24-year-olds—are actually watching TV far less: 2.7 hours a day, or about three-fourths that of their older counterparts. Games, social media, and short-form videos on YouTube account for a substantial portion of youth entertainment time. Surprisingly, so does reading.

Yes, reading is making a comeback. According to a report by the National Endowment of the Arts, reading rates have been on the rise since 2002.<sup>53</sup> And not just any reading: literature. People—especially younger people—are returning to stories: the 18- to 24-year-old cohort made the largest gains in reading, increasing by 9 percent between 2002 and 2008, and the trend has only continued since then. Millennials are the most widely read age group, with 87 percent of them reporting having read a book in some format—print or digital—in the past 12 months, compared with 73 percent of the general population.<sup>54</sup>

Whether we read on our phone, an e-reader, or in print, reading gives us an invaluable path to elsewhere. It's called "transportation": stories "transport" our minds out of our present environment and into something else. Since our earliest ancestors first discovered the joy of swapping stories around the campfire, there's been only one surefire way to transport ourselves: to hear a really, really good story.

Technology may be changing that. Through truly immersive technology—augmented reality and virtual reality—we may be able to achieve this sense of being transported not only without a gripping story, but without any story at all.<sup>55</sup>

"NOBODY IN HERE . . . THINK[S] IT'S ACCEPTABLE TO BE TETHERED TO a computer, . . . because we're all social people at heart. I think that a significant portion of the population of developed countries, and eventually all countries, will have AR experiences every day, almost like

eating three meals a day, it will become that much a part of you.”<sup>56</sup>

This is Apple CEO Tim Cook in a conversation with Senator Orrin Hatch at a technology conference in Utah. In Apple’s endless quest to personalize technology for its users, it’s now placing bets on a next-generation technology interface: augmented reality, or AR.

Most of us will likely have heard of Google Glass, the short-lived, groundbreaking gadget that put computers on tiny displays you could see out of the corner of your eye. It was revolutionary. It was the best tech development since the iPhone.

It was also a total flop—in its first commercial iteration, at least. One unfortunate side effect of the Google Glass nosedive is that it gave *all* AR a bad rap. To explore what AR really is, it’s first necessary to distinguish it from the product we most associate it with.

Google Glass sounded like science fiction come to life. Everyone could wear glasses that displayed features similar to those on your smartphone—just projected onto your glasses for you and you alone to see, with the real world perfectly in view in the background. The information you saw would depend on where you were in the real world. For instance, when you stepped outside in the morning, you’d see a weather notification with the current temperature. Walking down the street near your local laundromat, you might get a popup reminder that your dry cleaning was ready to be picked up. As you headed into the subway station, you could get a travel advisory warning you that the number-6 train was running with delays. Once you arrived at your subway stop, you could be shown turn-by-turn directions to navigate an unfamiliar neighborhood. And if you liked what you saw, you could take a photo with just a wink. Should you want to share what you were seeing with others, you could livestream your point of view directly from the glasses to the internet.<sup>57</sup>

Google Glass failed for several reasons, many of them marketing-related. When first rolled out, they weren’t available for sale to the general public, only to “Glass Explorers,” who had to pay \$1,500 for the privilege. They also creeped people out: the notion that someone stand-

ing in front of you might be looking at a display—or, worse, taking your picture without your knowledge—rather than making eye contact with you was deeply unsettling.

AR hasn't gone away, though. Instead, it's migrated to games. And here is where the kinks are being worked out to pave the way for mass adoption. The first wave of mass-AR use arrived with Pokémon Go. Yes, it's technically a kids' game. But it's also groundbreaking, raising public awareness about what AR is and can do in an easy-to-understand way.

The premise is simple: Download the Pokémon Go app on your Apple iPhone or Android device. Load the game. Then point your phone's camera at the path in front of you. By tracking your physical location using your phone's GPS, accelerometer, and compass, the game pops cute little animated creatures—those would be Pokémon—into your field of vision. You then have to physically approach them to “catch” them, which of course wins you points.

Pokémon Go marked the world's first mass-AR success. Around the world, more than 45 million users downloaded the game within the first days of its release in July of 2016. In the intervening year, the game was downloaded 750 million times<sup>58</sup>—equating to a stunning 10 percent of the global population. It's been heralded as the breakthrough tech for AR, just as the iPhone was for smartphones and Fitbit was for wearable health trackers.<sup>59</sup> Pokémon Go succeeded largely because users already had the device necessary to access it: a smartphone. You didn't have to carry around any additional gadgetry; you just had to download an app.

Apple's Tim Cook is betting on AR, as we heard in the earlier quote—not just thanks to the success of Pokémon Go, though it probably didn't hurt that iPhones were among the primary reasons for the game's massive success. Apple has partnered with several big brands, including Ikea and American Airlines, to promote the iPhone's AR capabilities<sup>60</sup> and has released a kit for app developers, the ARKit, containing tools to help them create new apps using AR.

While the AR market is still small, recall that the website market was small back in the 1990s too. It's only a matter of time before AR

use reaches a tipping point where any serious company will have to develop an AR-enabled presence. It may not be overnight. After all, the first handheld e-reader, the Rocket, was introduced in the late '90s, but it wasn't until Amazon launched the Kindle in 2007 that e-books really took off.<sup>61</sup> But all signs point to AR being at the forefront of the next phase of our relationship with technology products.

Immersion technologies such as AR matter because they represent a shift in how we experience reality. Pre-AR, we're already presented with different versions of reality when we go online: as noted earlier, the products Amazon displays to you are different from what they display to me; our news, Facebook, Twitter, and Instagram feeds are similarly customized. Even our search results are tailored: you and I could both Google the same keywords and end up with different results depending on "personalization" factors that include geographic location, search history, and the customized profiles created from our interaction with any and all Google products.<sup>62</sup>

With AR, we'll be able to see different images right in front of us, in the real world—though mediated through our phones. What's more, soon we'll be able to share what AR shows us with other users: in June 2018, Apple announced a new feature that enables users to share AR imagery between two phones.<sup>63</sup> We'll move from personalizing our online experiences with our handpicked network of "friends" to personalizing our real-world experiences with the same. While the present capability permits only two people to share an AR experience, there's no reason to believe this won't eventually scale to include groups as well.

C. S. Lewis wrote, "What you see and hear depends a good deal on where you are standing; it also depends on what sort of person you are."<sup>64</sup> As human beings, we already experience reality differently. Depending on our background, our values, our mood, and our state of physical wellness, you and I and someone else entirely may interpret the scene of a parade as exciting or overwhelming, as beautiful or depressing.

Technology won't be able to level the perceptive playing field for us; indeed, it will only further fragment what we see. In other words, we

already don't share the same *perception* about a uniform set of things in the world. Soon, with tech, we won't even *see* the same set of things in the world. We'll immerse ourselves in customized, personalized versions of reality that are unique to us and, perhaps, a select few we invite along for the ride.

Like it or not, immersion technologies such as AR will likely be at the center of the next stage in our relationship with tech. Not only will we wear our devices, but we will use them to filter what we see. Apple CEO Tim Cook doesn't see this as a bad thing. "AR has the ability to amplify human performance instead of isolating humans," he remarked.<sup>65</sup> AR's biggest success story, Pokémon Go, certainly seems to support this hypothesis. According to one study on the game's effects on users, the AR experience on one's phone is associated with "increased positive affect, nostalgic reverie, friendship formation, friendship intensification, and walking," all of which are associated with well-being.<sup>66</sup> All of this is to say that AR may well alter our sense of reality, but that new reality may equate to a really good time.

IN NEAL STEPHENSON'S AWARD-WINNING 1995 SCIENCE FICTION novel *The Diamond Age: Or, a Young Girl's Illustrated Primer*, a destitute young girl accidentally gets hold of an interactive virtual reality (VR) "book"—a primer—intended to train an aristocrat's daughter on how to comport herself in the upper echelons of their world. The book "grows"—becomes more complex—as the girl ages, adapting to her intelligence, her curiosity, her emotions, and her experience. Lots of other stuff happens, but for our purposes, let's just focus on the primer itself.

Immersive technology that adapts to our every need is not a new concept (think of the holodeck on *Star Trek* and the training modules in *The Matrix*), but the fact that the idea keeps coming back in story after story reveals something about human desire. We seem to long for our tech to not only entertain us, but train us. But there's a catch: it must be in exactly the right modality for each of us, personally. This tool

would feed us the precise experience and challenge to advance us to the next level of expertise, of ability, of comprehension—a “gamification” of learning that allows us to level up all the way to enlightenment.

Perhaps no other technology outside AR and VR has ever held as much potential to meet this desire. As VR filmmaker Eugene Chung noted, “We’ve effectively had the same flat screen medium since 1896. VR/AR uniquely provides a sense of presence and immersion; it’s a brand new art form and brand new form of experiencing.”<sup>67</sup>

Immersive tech is not being developed just for gamers and niche markets. Tim Cook describes AR as potentially game-changing for everyone’s everyday experience of technology, just as the iPhone was. “The smartphone is for everyone,” he reported in a 2017 interview with the *Independent*.<sup>68</sup> “We don’t have to think the iPhone is about a certain demographic, or country or vertical market: it’s for everyone. I think AR is that big, it’s huge.” Apple is putting significant money behind this sentiment. In the spring of 2018, reports leaked of an Apple headset in development that would facilitate both VR and AR. With Apple’s characteristic commitment to visual aesthetics, the leaked plans describe an 8K resolution display per eye—for context, this would be a higher resolution than the best TVs on the market today.<sup>69</sup>

Whether Apple’s headset, slated to come out in 2020, will allow us to truly immerse ourselves in another reality—one that’s vivid and complex and that *feels* real—has yet to be determined. But given how life-altering our current form of immersive technology is—introduced to us through Apple’s iPhone—it’s possible that this company has what it takes to produce yet another mass-magical tech moment with its AR/VR device: the ability to become fully engaged not in one’s physical surroundings, but in one’s mental experience. Whether this will ultimately be good for us is almost impossible to predict; what we *can* predict is that such technologies are coming. We should be prepared for what could be the next great unknown tech-mediated life-changer.



## EIGHT



# A DECLARATION OF CITIZEN-USER RIGHTS

It's time to take 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. This chapter gives us options for how to reconcile our feelings of disempowerment via tech with the feelings of being empowered by it at the same time; it explores what we as citizen-users must do to ensure that we remain actively engaged in the development of net states, monitoring their relationship with our nation-states and with our own lives; and it offers a citizen-user pact with net states.

In 1948, only 82 independent sovereign nations ruled the world—113 fewer than there are today—thanks in large part to colonialism. And the countries that did exist were unstable and weakened: the Second World War killed over 55 million people through conflict, disease, famine, and other war-borne causes. It took a devastating toll the world over.

While the war formally ended in 1945, the years following were far from peaceful. The Soviet Union, which had lost a staggering 27 million people to the war, quickly consolidated power by occupying the neighboring countries that had fallen to shambles following the Ger-

man invasion: Poland, Czechoslovakia, Hungary, Bulgaria, Romania. In 1946, British prime minister Winston Churchill called these Soviet postwar occupations the lowering of the “Iron Curtain,” thus describing what would become a 45-year-long Cold War between the Soviets and the Western world—former allies that had fought alongside one another just one year prior.

Over the next few years, the world only grew more complicated. In January of 1948, Mahatma Gandhi was assassinated. In May, the United Nations recognized Israel, at which point Egypt, Jordan, Syria, Lebanon, Iraq, Saudi Arabia, and Yemen attacked, setting the tone for 70 years of hostilities in the region. In June the same year, the Soviet army blockaded Berlin, preventing the delivery of supplies through all roads and rails and fanning the flames of the nascent Cold War. The government of South Africa, also that year, launched a policy of apartheid, creating an institutional system of discrimination that would plague the country for the next almost 50 years. In short, the world was a disorderly and dangerous place.

Despite this, the majority of countries did agree on one thing: the atrocities of World War II, a war in which more civilians were killed than uniformed soldiers, had to be prevented from recurring at all costs. The world needed rules for war to safeguard the innocent and to protect fundamental rights. This gave rise to the Universal Declaration of Human Rights in 1948 and the expansion (from multiple earlier forms) of the Geneva Conventions in 1949.

Unlike the Geneva Conventions, which set out the rules and conditions for “humane” conduct during wartime, the Universal Declaration of Human Rights wasn’t legally binding, making its success all the more astonishing. It was, at the time, almost like a formal suggestion, albeit a powerful one. It enumerated minimal rights that should apply to every living person on Earth.

On December 10, 1948, for the first time in history, dozens of nations committed themselves to a pact not to other nations, but to humanity itself: acknowledging that regardless of nation of origin or citizenship

or religion or any other factor, humans anywhere and everywhere, from the moment of birth through their last breath on Earth, possessed intrinsic rights. And with this document, the idea of people having rights that supersede and exist independent of any particular nation-state bloomed into life.

There is no net state equivalent to the United Nations—no body where net state leadership can come together and question whether the application of their products and services will ultimately serve to make the world and its citizens a better place. Absent that body, there's no pact defining standards and protections that members adhere to.

This chapter argues that there should be: our world needs a pact that establishes citizen-user protections from net states; a set of principles that guide net state developers in becoming better stewards of the digital ecosystem (more later on just what that ecosystem is).

Protective pacts generally reside in the realm of the nation-state—either individually, through a constitution; or multilaterally, through documents such as the Geneva Conventions. Before turning to what a pact between net states and their citizen-users might look like, it's worth taking a look at the pact already familiar to most of us: the US Constitution with its Bill of Rights.

TEDDY ROOSEVELT IS ONE OF AMERICA'S MOST FAMILIAR AND MOST beloved presidents. In one ranking of past presidents, Roosevelt came in second only to Abraham Lincoln.<sup>1</sup> Roosevelt was one of the most literary of all presidents, writing 35 books in his lifetime. He was also one of the most idealistic, devoting his considerable writing talent to urging his fellow Americans to live principled, "strenuous" lives.

On government, he held particularly strong views. In a 1902 speech to thousands of citizens gathered in what is now Pack Square Park, a tree-lined, open-air meeting grounds in Asheville, North Carolina, Roosevelt spoke about the need to heal the wounds from the Civil War.<sup>2</sup> He called upon Americans to do so by becoming active participants in their

democracy, saying, “We get in the habit of speaking about government as if it were something apart from us. Now, the government is us—we are the government, you and I. And the government is going to do well or ill accordingly.”<sup>3</sup>

If we, the people, are indeed government, who does that put in charge? It turns out that both conceptually and actually, the American government does have a boss—and it’s not the president. Government is both empowered and restrained by the US Constitution: it can do only what’s been outlined in this document. Of course, Congress has passed many laws since the ratification of the Constitution back in 1789, but none of them can override the Constitution itself. The American government serves the American people, according to the rules detailed in the Constitution, not the commander in chief: even he or she is beholden to the Constitution.

The president and everyone else who works for the American government has, then, five basic responsibilities that are detailed in the Constitution’s preamble: to “establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity.”

The first three responsibilities don’t tend to be terribly controversial. As a people, Americans largely support the idea of the rule of law: 68 percent of Americans trust the judicial branch of government, a far higher amount than those who trust the executive (45 percent) or the legislative (11 percent).<sup>4</sup> Americans generally prefer a peaceful and orderly society over, say, anarchy. Americans also really like the military, with 74 percent trusting that it will keep them safe. But the final two—to “promote the general welfare” and “to secure the blessings of liberty”—are harder to define and much more difficult to find consensus on.

There are exceptions: as regards “liberty,” 85 percent of Americans believe in the freedom of speech. In fact, so important is this particular freedom to Americans that 73 percent report they would be willing to die to defend it.<sup>5</sup> In the liberty department, Americans are generally content: 87 percent report having a lot of freedom in their lives.<sup>6</sup>

While we may be happy with the degree of freedom we enjoy, this doesn't tell the whole story of American happiness. Because Americans aren't actually doing all that well, as a people.

We're in greater danger than we used to be, for instance. Life in the United States is less predictably safe than it was twenty years ago. As discussed previously, part of the reason for this is the epidemic of gun violence: from 1995 to 2005, there were 112 mass shootings in the US.<sup>7</sup> In the decade from 2006 to 2015, there were 310 mass shootings: a 176 percent increase. In 2018, there were 340 mass shootings: an average of 28 a month.

Drug overdoses are up, too. Overdose fatalities from opioids were five times higher in 2016 than in 1999.<sup>8</sup> It's a widespread problem: in 2016, 26 states saw a statistically significant increase in fatal drug overdoses. And it's getting worse: by 2019, 130 Americans died each day from opioid overdoses.<sup>9</sup>

Suicides are also up. Death by suicide is now the 10th leading cause of death in America.<sup>10</sup> And there's been an especially troubling recent spike among young people. From 1950 to 2014, death by suicides among 15- to 24-year-olds increased by 255 percent.<sup>11</sup> Among even younger children—those 5 to 14 years old—suicides increased by a heartbreaking 500 percent.<sup>12</sup>

Americans are not doing all that well as a democracy, either. As noted earlier, we don't trust our government. Very few of us vote. And increasingly, we can't even tell facts from falsehoods in the news. We *feel* free, at least, and we're proud of that. But on balance, we as a people and as a citizenry are less *well* than we used to be.

This isn't just an American problem. The world is, in many ways, unwell. Democracy, once a seemingly inevitable form of governance spreading across the globe, is suddenly in decline.<sup>13</sup> Attacks on a free press are on the rise in authoritarian states and major democracies alike.<sup>14</sup> We've seen an overall loss in global freedoms for eleven consecutive years, thanks to what the human rights watchdog organization Freedom House calls a "crisis in confidence in democracies," along with

a rise of populist and nationalist movements fueled by antiestablishment politicians.<sup>15</sup>

In 2017, survey respondents from 145 countries reported feeling more worried, stressed, anxious, angry, sad, and physically in pain than at any point in the previous decade.<sup>16</sup> Depression is on the rise: the World Health Organization (WHO) reported global depression rates spiking starting in 2005—not coincidentally, I argue, around the same time that time Facebook (2004), YouTube (2005), and Twitter (2006) hit the scene. And it's only gotten worse: after years of stagnation, from 2005 to 2017 rates of depression leaped up 18 percent. Depression has become so widespread that in March 2017, WHO declared it to be the number-one cause of illness worldwide.<sup>17</sup>

As developed as we are technologically, we (as a people) are on the edge of an epidemic of bad feeling. There's been plenty written about excessive social media usage exacerbating depression—a phenomenon dubbed “Facebook depression.”<sup>18</sup> But I argue that there's more to what's happening than just heightened FOMO (“fear of missing out”) or the negative impacts of cyberbullying, though those are problems in their own right.

I contend that we are experiencing a mass sense of cognitive dissonance. We feel both empowered and powerless by the same tools, at the same time.

Net states matter here, because they provide us with the tools to enhance our sense of freedom—the one thing we've really got going for us. But as we've seen, just because they make us feel free doesn't mean that they don't come with a cost. We are empowered by the devices that give us the world's answers at the touch of our fingertips. Yet we feel powerlessness to do anything about what personal information is collected in the process. We are empowered by our incredible increase in awareness about what's going on in the world, thanks to the massive amounts of media we consume each day. But we feel powerless to do anything to stem the tide of terrible things we read and hear about. We are, in feeling and in fact, more cognitively powerful—we can see more, find more,

learn more, connect more—than we’ve ever been at any point in our history. Yet we’re paralyzed, unable to engage in meaningful action; our attention is drained, our bandwidth exceeded; our emotions and cognition are overloaded and exhausted.

We can’t persist like this. We risk being—or worse, risk our children being—drugged, depressed, or suicidal. While the causes for our drug use, depression, and suicidal urges are complex and multifaceted, there’s no escaping that one of the most obvious correlations in the rise in all three is the simultaneous rise in our technology use. The more we use tech to excess, the more drugged, depressed, and suicidal we’ve become. The more media we expose ourselves to through technology, the more we feel beaten down by the incivility we see in partisan politics—in Washington, DC, yes, but also among the acquaintances in our social networks.

Take, as just one example, Russian misinformation warfare during the 2016 election. We know more about it than we ever could have, pre-social media. Yet we don’t see action on the part of our elected leaders to protect the 2020 election from similar warfare. And we don’t feel as if we can do anything about it on our own. Given so much awareness and the feeling of so little power to effect change, it’s no wonder we feel terrible.

Our world is nowhere as dismal and chaotic as it was just after World War II. But we’ve been experiencing our own version of hell ever since the Global War on Terror was unleashed almost two decades ago—that is, when we’re not too distracted, exhausted, or depressed to think about it. Our particular fight, here in the United States, is diffuse, protracted, and unpredictable; it is both land-based and cyber; it is also distant and surreal. We Americans may even feel guilty about the fact that it feels so far removed, if we even remember that it’s still happening. And if we do remember, that’s a sure path to feeling awful, because terrorism is incredibly scary. Here, as with the Russian misinformation campaign, we feel powerless to do anything to change its course. We’re in what feels like an endless war—multiple wars, if you count the onslaught

of cyberattacks on our country: 4,000 a day, according to the FBI.<sup>19</sup> It's almost impossible to conceptualize it all, let alone feel as if we can be part of the fight.

There's no silver bullet for our problems. We can't fix all the world's ills. But some component of our sense of powerlessness lies with our (simultaneously empowering) technology, and I do have a suggestion to address that.

We do not need to feel powerless. We are not, in fact, powerless. We need to remind ourselves and the keepers of our digital realm of that. We need, as once in a while the world seems to need, a declaration: a set of suggestions that establish ground-floor, foundational conditions that should apply to every human being on Earth.

We need to establish a new relationship with our net states; one that reclaims power that users can exert over their own data, their sense of privacy, and their experiences of the digital ecosystem. We need a pact that puts citizen-users at the center—a digital descendent of the Universal Declaration of Human Rights, a tech-savvy version of the Constitution's Bill of Rights. We don't need any more terms of service. We don't need Bible-length provisions to counter the unreadable terms net states provide us. We need just a few basic principles—brief but unassailable fundamentals that everyone should be assured. We need a Declaration of Citizen-User Rights.

The goal of such a pact—not an agreement that *net states* write and users must accept, but rather an agreement that *citizen-users* craft, enumerating rights we expect to be respected—is to create a set of ground rules that net states must agree to in exchange for our using their products: specifically, in exchange for our data and our attention.

To figure out how to create such a pact, we can look to several precursors, road maps for what a meaningful pact between net states and users could look like. The Cybersecurity Tech Accord (aka the Digital Geneva Convention) described earlier may seem like a likely candidate. But for all its laudable qualities, it's actually not the best model for what citizen-users need for their protections among net states. The Digital

Geneva Convention gets a lot right. But the main issue is that it's not really *for* users. It's a pact *by* net states *for* net states. Users are among the objects of the pact, but they're not really a party to it; only the net states are.

Before we can craft a user-centric declaration, let's quickly review the current state of affairs with what we've already signed on to.

Everyone who uses technology is already party to multiple versions of terms of service (TOS). But these, too, aren't *for* us; they're for tech companies to protect themselves from liabilities. They're the gate through which we must pass to use a company's products and services. So we agree to them, time and again, without reading them. Even if we did read them, we'd discover that they don't put us—the users—and our protections front and center. The focus is on the tech company itself, ensuring that it doesn't get sued when it eventually shares your data with third parties.

There are various websites that attempt to help users navigate which platforms and services have TOS that are more or less risky for the user. For example, the website Terms of Service; Didn't Read, or TOSDR (a play on "too long; didn't read," generally shortened to TLDR, which refers to online content that people caution they didn't bother reading), was launched in 2012 in collaboration with the Electronic Frontier Foundation (EFF). It classifies sites depending on their risk to users, from A to E. (The search engine DuckDuckGo gets an A since it doesn't keep track of search queries; YouTube gets a D, mostly because it keeps deleted videos for its internal purposes, unknown to the user who created the content.) The rating of TOS is a collaborative effort: users from all over the web note changes to TOS on GitHub, one of the most widely used code-sharing platforms. But this also means it's uneven—without armies of online volunteers, it's difficult to assess how "good" TOS are for users. TOSDR does helpfully compile various TOS into a single location with plain-language summaries. Even if out of date and far from exhaustive, its list is still quite instructive (as are those of other sites).

To see if I could flesh out what was missing on TOSDR, in August of

2018, I compiled and read all the terms of service for Amazon, Apple, Facebook, Google, Microsoft, and Tesla. Here's what I found.

First, there's a wide range of "average" when it comes to the sheer length of terms of service.<sup>20</sup> (Note: for the purposes of this exercise, I examined only language explicitly called "terms of service"—not ancillary policies, such as those mentioned in FAQ or other legal policies listed; in other words, I stuck to the agreement between the user and the platform or service.)

Apple's iTunes TOS section is a handful, adding up to around 6,804 words.<sup>21</sup> Google embraces brevity (and ambiguity—more on that shortly), with its TOS clocking in at about 1,869 words.<sup>22</sup> Facebook is somewhere in the middle, at 3,243 words.<sup>23</sup> Amazon is about the same, at 3,387.<sup>24</sup> Microsoft blasts the others out of the water for length, at 15,290 words.<sup>25</sup> Tesla covers their business in 5,736 words. All this averages out to terms of service composed of 7,265.8 words for your standard net state. Even if these terms were written in plain English, as many of them now are (thanks to the need to comply with the EU's General Data Protection Regulation), if the average person reads 200 words per minute, it would take 36 minutes to read one single platform's terms of service; 3 hours and 20 minutes for all the ones I calculated—just six of zillions.

In practice, we not only don't want to spend this much time reading TOS, we come across too many to realistically do so. Researchers at Carnegie Mellon University estimated that we encounter 76 sets of terms of service in a year, based on our 2008 browsing habits<sup>26</sup>—back when we spent only 13 hours a week, or 1.8 hours a day online.<sup>27</sup> Terms of service are shorter now—again, thanks to the EU's GDPR. But we're still encountering them quite regularly. In 2016, it was estimated that we spent 10 hours and 39 minutes per day consuming media in some form—via our smartphones, TVs, computers, tablets, e-readers, and so on.<sup>28</sup> Our attention, as discussed in chapter 7, is a precious commodity. We try hard not to waste it; we spend only 10 to 20 seconds per web page to evaluate whether it's worth our time before moving on to the next one.<sup>29</sup>

If we can barely pay attention for the 10-plus seconds it takes to see whether or not we want to stay on a web page, the notion that we'd take 36 minutes to peruse a boring user agreement—76 times a year, no less—is simply unrealistic.

And our net states in question? There are six we've been looking at, as you know. But they're not just six companies; they're six *parent* companies, and collectively they've acquired 673 other companies, according to transaction data publicly available through Crunchbase. Many of the acquired entities are likely irrelevant to us: Apple bought lots of hardware component manufacturers, for instance; Facebook, lots of messaging startups. But many of them are significant entities that we run into on occasion, though we may not be aware that they're owned by a major net state: Instagram and WhatsApp (owned by Facebook); Skype, LinkedIn, and Nokia (those are Microsoft's); IMDb and Zappos (Amazon bought those); YouTube, Waze, and Zagat (all Google's), to name just a few. And they all have *their* own terms of service as well. Indeed, if we were to map out the universe of the net states and their 673 acquisitions, I'm fairly certain we'd discover that there's no way to both be active in the digital sphere and avoid having to agree to terms of service informed by one of the major net states.

In sum, if we're online, we are bound to our net states, in some way. We've given ourselves over to them, without even knowing what that really means. We can't put this particular genie back in the bottle—the data we've set free has likely passed through so many third parties at this point that it would be virtually impossible to suck it all back in. But we can make a decision to change how we handle our data moving forward, to reclaim power over what we give out, to whom, and for what purposes.

LET'S START PRACTICALLY. HERE ARE THE MAJOR AREAS COVERED IN this book's big-six net state terms of service: (1) your data when you use their product/service; (2) your data once you leave their product/ser-

vice; (3) your expectation of privacy while using their product/service; (4) the ground rules about using their product/service; and (5) what access third parties have to your data.

The reason to start with existing areas in the terms of services is that the ultimate goal for crafting a Declaration of Citizen-User Rights is to be a viable challenge to the TOS that net states create. Thus we can't ignore their areas of concern. But instead of focusing on ensuring that the net states don't get sued, *our* document—a set of universal “terms of rights”—will ensure that citizen-users don't get taken advantage of.

First, some general observations on terms of service. Based on those that I examined, they tend to be an umbrella set of conditions users must agree to. Yet despite their length, they don't come close to laying out all the details—especially some of the details users are likely most concerned with. For example, all six net state TOS that I reviewed directed readers to a separate “Privacy Policies” document that users were encouraged, but not required, to read. *These* are the policies that really get into detail about what they're doing with our data. By including a blanket statement in the TOS along the lines of, “By accepting this agreement, you're also accepting our privacy policies, which you can read here [click here],” companies effectively shuttle their privacy policies even further out of users' reach.

I'll spare you the mind-numbingly boring details. Here's the upshot, which isn't great news but no surprise: if you use any product or service of the six major net states, you don't really have any privacy online. Your data will be kept, analyzed, and shared with or sold to third parties, as they see fit. One notable exception is Apple, sometimes: whatever data is on your phone remains on your phone, not on Apple servers—unless you enable automatic syncing with iCloud. This is one of the reasons iPhones bedevil law enforcement officials: there's no “back door” where Apple can unlock someone's phone, remotely or in person.<sup>30</sup> If you use a strong password—meaning, not the word “password” or “1 2 3 4 5 6,” which remain the two most common passwords, amazingly—it's really, really hard for anyone to break into your phone.<sup>31</sup>

The data collected *while* using your phone is all tracked of course. Facebook notes, for instance, “We use the data we have—for example, about the connections you make, the choices and settings you select, and *what you share and do on and off our Products*—to personalize your experience” (italics added).<sup>32</sup> This means that if you have Facebook open on your phone and then open another app, Facebook will collect data on what you’re doing on that app, too. *All* the net states (and tons of other companies, too) share or sell—also called “licensing”—your data with unnamed “third parties” as they see fit, for which you have granted them “worldwide” permission, according to their TOS. Amazon goes so far as to say that they’ll also share or license your name in addition to your data, if you’ve ever posted a review or comment.<sup>33</sup>

In short, our data online is pretty exposed. We *say* we care a lot about it—a Pew poll in 2016 reported 75 percent of us as saying privacy is “very important” to us.<sup>34</sup> But we do precious little to actually protect our privacy online. Almost all of us—91 percent—accept TOS without reading them (the figure is closer to 97 percent for millennials).<sup>35</sup> Claiming to care about privacy but not taking action to protect it is such a widespread phenomenon that researchers have dubbed it the “privacy paradox.”<sup>36</sup>

The most plausible explanation I’ve seen that explains this paradox has to do with our squishy sense of time.<sup>37</sup> Our worries about privacy—a breach, a leak, an abuse of our data—are focused on something possibly happening *in the future*. The future’s an abstract concept; it’s difficult to visualize in a tangible way. On the flip side, the actions that put our privacy at risk are *in the now*. We’re getting something immediately—access to information, a platform or service, the ability to connect, see photos, receive updates. We get visceral, tangible, right-now representations of our friends, our frenemies, our crushes, our curiosities. All you have to do is sign away your privacy with the click of a TOS “accept” button and bam! You’re in; you’re connected to the object of your desire, whatever that may be. But taking the time to be careful about your privacy takes, well, time—a lot of it—as well as that prized commodity,

your attention.

So here's what I propose. We take the time, in these next few pages, to negotiate a better deal for ourselves. I'm not a lawyer, but then I'm not suggesting anything legally binding. Rather, let's set out a few simple, high-level terms that protect users in principle; the lawyers can duke it out and pretty it up some other time. Our focus in the Declaration of Citizen-User Rights is to address the meat of the problem: how to reclaim the right to our privacy—and our sense of power—without having to sacrifice the benefits of technology.

The goal with these rights is not to codify *tactics* for user protection against technology's ill effects—for example, steps to turn off location-tracking on your phone or to prevent your contacts list from being uploaded without your permission. For these sorts of protections, the previously mentioned Center for Humane Technology, founded by former Silicon Valley leaders, provides excellent resources. The goal here is to identify the fundamental rights that users would need to claim to substantively alter the balance of power between us and net states. There are likely dozens of possible rights. Let's start, though, with the three rights poised to make the greatest impact on our lives, expressed here as three principles. Those principles alone make up the Declaration of Citizen-User Rights. They are: Citizen-users have the right to choose how they pay for their own content privacy. Citizen-users have the right to delete their own content from the public record. And citizen-users have the right to know how their data is being used. Now let's look at each of these principles in turn.

### **#1. Citizen-users have the right to choose how they pay for their own content privacy.**

This first principle may seem counterintuitive. Like, why should we pay for something that's already ours? It's *our* information, after all.

While understandable, that argument isn't going to help. We're so

far down the road of information-giveaway—since the dawn of the information age, really—that tech companies would have to reinvent their entire business model to simply stop collecting our data if they got nothing in return. Also, to repeat a quote from Google Jigsaw’s Scott Carpenter, “Most tech companies are just trying to get off the mat and into the game.” The six net states featured in this book are über-rich, but the vast majority of tech companies are barely scraping by. It’s simply not viable to operate a business that gives away a free product or service if the provider doesn’t get anything of value back from the user.

For a long time, this thing of value was our data. Our privacy. Our sense of power. What I’m suggesting is that we redefine what’s valuable. If our data, privacy, and sense of power are precious to us, then we need to offer something else that’s valuable. And just about everyone values money.

Here’s what we’d get: walls—borders protecting our content. The photos, videos, and text we put online would stay on our chosen platform and that platform only—no sharing, licensing, selling, or in any other way permitting access of that data to unidentified third parties. As it stands, those third parties underwrite the cost for our free access to platforms and services. So in exchange for keeping our data nice and snug on a single net state’s system, we as users would have to pay for those walls.

It may not be an immediately attractive notion: demanding the option to pay money for something that’s currently free. But remember, it’s not *actually* free—we’re paying with our data. Therefore, I suggest that Amazon, Apple, Facebook, Google, Microsoft, and Tesla—and any other tech company large enough and wealthy enough to adopt this option without it breaking their ability to do business—provide users with a for-pay option for any service in which our personal data currently serves as payment.

This is not an unusual business model. It’s how cable TV works: we pay for it, and in exchange we’re not forced to watch advertisements. Streaming music services like Pandora work like this as well: there’s a

free version, with advertisements. But if you pay for the service, you're not subjected to the interruption of ads.

What I'm proposing goes beyond simply saying that net states should create an option whereby users are invited to pay for a particular service. We're talking about fundamental *rights* here. This first principle suggests that we have the *right* to demand a for-pay service. We have the *right* to declare our data sacred and offer something else of value in return. We have the *right* to demand that our data goes in a vault.

The company itself can still access the data: learn from it, develop products from it, use it to improve their services. But in exchange for our usage, the company would have to agree not to share or sell that data with any unidentified third parties.

This creates a few problems, unfortunately. In a society like ours, where the gulf between rich and poor is already vast and growing vaster, a for-pay option might seem affordable only to the well-heeled. This would leave the struggling lower socioeconomic classes at an even greater disadvantage: they'd still be losing out on personal privacy, while the rich could protect theirs.

Yet, even people without a ton of money do tend to pay for things they really value. As was noted earlier, 77 percent of Americans own smartphones and 73 percent of American households have broadband internet access, for instance.<sup>38</sup> Privacy, like phones and internet, might turn out to be so valuable that it's deemed affordable even by those with few financial resources.

Here's what the financial impact of the internet-for-pay option might be. The median American household income in 2016 was \$57,617. Income varies significantly by state, of course, but that was the nationwide average.<sup>39</sup> Calculating how much of that gets paid in taxes also depends on many variables, like your marital status, whether you have dependents, and what state you live in. But let's take what we know about federal, state, and local tax rates and ballpark the average tax rate for the average American to be 17 percent.<sup>40</sup> That would put the average American's take-home pay at about \$47,800, or just under \$4K a month.

As noted earlier, in 2017 cell phone bills were an average of \$80 a month, while broadband bills ran somewhere around \$60 a month.<sup>41</sup> This means that even without accounting for the cost of our actual devices—phone, laptop, television, tablet—we’re spending around \$140 a month to be digital citizen-users.

Apple and Google Drive (where you can store files in the cloud) already have services that cost money: you can stream unlimited music from Apple for \$10 a month, for example, or store gobs of data on Google Drive for \$2 a month.<sup>42</sup> In other words, for-pay tech services that already exist don’t cost a ton of money. If each of the major net states charged just \$5 a month for their privacy-enabled for-pay tier of service, (1) they’d make an absolute fortune, which sounds like an incentive to create such tiers, and (2) we, the citizen-users, would be buying back our data, our privacy, and our sense of power for the cost of muffin and a Frappuccino at Starbucks.

However. There’s another problem with this very transactional approach to our privacy, a more principled and foundational one. What I’ve suggested is a pragmatic approach that looks forward, forgetting about all the data that has already been taken for free and focusing on the future data that we can protect. But there’s another argument that we need to contend with—beyond whether it was ever okay that our data was so freely trafficked without our actual consent (not TOS consent, but conscious, reflective, I-know-what-I’m-getting-myself-into consent).

And that is this: “Information wants to be free.” Free and freely shared. It’s one of the founding principles of the internet, as we’ve seen; the central tenet of the tech ethos.

What happens to the European Union’s internet experience in light of the General Data Protection Regulation (the GDPR, discussed in chapter 3) will be instructive in seeing how this plays out. Users in the EU can invoke their “right to be forgotten,” effectively removing their digital footprint from search engines’ reach. The question becomes: If we kept our personal data private, would our global internet experience still be full and rich and diverse and accessible, or would the internet become

a different place, showing us only the content that users couldn't afford to pay to keep private? Would the internet as we've experienced it effectively shrink and wither, becoming a less vibrant, democratic, and diverse hunting ground for information and connections than we have today?

Unclear. But the status quo—in order to be digitally active, citizen-users have to relinquish their right to privacy—cannot be sustained. Principle 1 is our best option for creating a viable workaround to the privacy issue: one that both net states and citizen-users could benefit from.

## **#2. Citizen-users have the right to delete their own content from the public record.**

Think of this principle as the clean-up clause. It will make more sense with a bit of background. The European Union's General Data Protection Regulation made a bold statement, as we saw earlier, with respect to users' online information. Instead of focusing on the information itself, it focused on the person: the "data subject." In so doing, the entire set of legislation shifted our attention from *content* to *humanity*: "subjects," defined as "people who live in the territory of, enjoy the protection of, and owe allegiance to a sovereign power or state." In the case of the GDPR, the subjects are enjoying the protection of and owe allegiance to the European Union, which, in turn, oversees their protection. And not just generally, but in a very specific area: their data.

In this book, I've used the term "citizen-user." Why not just say "data subject"? Why introduce yet another term into the mix? Two reasons. First, I'm referring not to citizens of a single country, but *all* people who use digital tools and services. Second, I took my cues from Microsoft's Digital Geneva Convention—aka the Cybersecurity Tech Accord—which refers to people as "users," "customers," "civilians," and "citizens." The accord makes it clear that signatories are protecting users *and* customers *and* civilians *and* citizens, regardless of the country in which those

individuals reside. I could have called us all “user-customer-civilian-citizens,” but that felt a little unwieldy. Hence, citizen-users: “citizen,” because we have a responsibility to be active participants in the power structures in which we function; and “users,” because we don’t physically inhabit the digital ecosystem. Rather, we *use* its tools and services. Those same tools and services—the products of net states—*they’re* the things inhabiting the digital ecosystem. We citizen-users are visitors; at times, cruising through; at times, veritable squatters—but only and always transitional actors.

If the digital realm is an ecosystem that we improve or degrade through our presence, principle 2 ensures that it remains a place we’d want to be. Think of a park: it’s more fun to have a picnic in a clean park than one strewn with litter; therefore, it’s our responsibility to clean up our own litter.

Principle 2 proposes that we claim the right to improve what our presence online does to the overall quality of the place. I am in no way suggesting censorship. If someone criticizes an article I wrote, I shouldn’t be able to delete that criticism just because it irks me. However, if I realize that this criticism is valid, that I advanced a line of thinking that wasn’t supported by facts and data or was just plain wrongheaded, I should be able to correct my mistake and take that article down. Such action would be a form of informational pollution control, like cleaning up the mess you make after that picnic in a park. The evidence that I wrote something dumb would remain—in the form of whatever criticism was posted about me. But I would at the very least be able to retract the original, offensive material and thus keep from negatively impacting future readers.

The GDPR has a similar provision in its “right to be forgotten” (RTBF) clause. That clause doesn’t broadly stipulate that any data subject can demand that any and all content about them be removed from, for example, Google. No, the “right to be forgotten” is balanced out with the “right of freedom of expression and information”—which is, granted, open to interpretation—and with the public interest, such as if certain

data is necessary for “legal obligations, for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes.”<sup>43</sup>

It turns out the wiggle room under what’s considered to be in the public interest or of research value is fairly broad. In the first year Google processed RTBF requests, it decided to retain 58.2 percent of URLs requested to be taken down<sup>44</sup>—taking down only about half a million links. The indexable internet (the portion that search engines like Google can find) contains roughly 4.44 billion web pages.<sup>45</sup> Even if Google took down half a million web pages each year—roughly 1,369 web pages per day—we’re posting several hundred thousand times that amount in new digital data: approximately 1.5 million new websites a day.<sup>46</sup> Even if only 4 percent of those 1.5 million websites can be found on Google, the fact remains that there’s a staggering amount of new content that we *can* find, almost all the time. Judiciously removing 1,000 or so links a day—one-third of which link to personally identifiable directory information, according to the registry of removals in the EU—would be like extracting drops of water from an ocean; it would barely register as a ripple.<sup>47</sup> Granted, if the one page you’re looking for happens to be one of the pages that’s no longer online, it’d be frustrating. But still, it’s a worthwhile tradeoff to ensure that you regain control over your data, your privacy, and your power.

### **#3: Citizen-users have the right to know how their data is being used.**

Think of this principle as similar to the US 1967 Freedom of Information Act, or FOIA, for net states—with a twist.<sup>48</sup> FOIA is the law that lets citizens request that government agencies share a copy of their information with the public. Of course, you have to first know what information to ask for. A request like, “Send me all your emails!” sent to all government agencies will likely be ignored. A request with specific parameters, like,

“Send me any email traffic pertaining to Benghazi, Libya, from August 2014 to November 2014,” sent to a specific agency, such as the United States Mission to the United Nations, is more likely to be processed.

FOIA isn’t a perfect system; it can take a few months to get a response. Yet regardless of how clunky and slow it may be, this transparency process exists. And it gives citizens power to review information that their government—whose work they fund through their taxes—produces.

Here’s where principle 3 differs from FOIA: it’s not just a request for information. Most net states will already let you gain access to the information they have on you. For example, you can download all of your previous Google searches or Facebook posts with a few clicks. But principle 3 states that net states also have to let you know *what they’re doing* with the information that they have on you. If they’re sharing it with marketers for the purpose of better targeting you with ads, say so. If they’re licensing it (remember, a friendly way of saying “making money off of it”) with data brokers for the purpose of contributing to some third-party profile on you, say that. And users should have the right to opt out of certain practices, especially if they’re paying for services, as outlined in principle 1.

This issue is also covered in the European Union’s GDPR in its “right of access.”<sup>49</sup> Not only do tech companies have to let you know what data they have on you, the GDPR requires them to tell you what they’re doing with it—“the purpose of processing”—as well as anyone else they’re sharing it with: “Any third party recipients of this personal data, both backward or forward looking, especially recipients in third countries.”

What this means in practice is that anyone in the EU can ask any company—including the company they work for—to hand over any documents that refer to them, including private personnel records and other potentially sensitive materials.<sup>50</sup> Companies have 30 days to comply or face paying a substantial fine—up to a walloping 20 million (roughly \$23.6 million) or 4 percent of the company’s total worldwide annual turnover of the preceding financial year, whichever is higher.<sup>51</sup>

While this sounds like a huge victory for citizen-users on the face of it, it creates significant complications for companies. For instance, the General Practitioner Committee of the British Medical Association, representing 160,000 members in the UK medical community—urged members to petition their local officials highlighting “unintended consequences” of the subject access requests specifically.<sup>52</sup> The petition notes that by requiring physicians to review every page of medical records to ensure that no prohibited information was being shared, they were losing on average an hour a day reviewing paperwork—an hour they formerly would have spent “caring for sick patients.”<sup>53</sup>

The subject access requests aren’t just a time issue; most companies wouldn’t know where to look for all the data requested. An astonishing 82 percent of companies surveyed admitted that they didn’t know where in their own companies their critical data was located,<sup>54</sup> what with data being stored on individual workstations instead of (or in addition to) a centralized database, in email inboxes, or in multiple databases or documents within the organization that aren’t connected or communicating with each other. While “Big Data analytics” are all the rage conceptually, in practice a lot of companies are still playing catch-up to understand even the very basics about their data, like what they have and where it’s stored. How to mine it for useful insights is a whole different level of complexity that many companies are still only dreaming to reach.

But the inability of companies to find data—a real and immediate challenge—is no reason for citizen-users not to exert their right to know how their own data is being used.

MOST OF US PROBABLY FIRST ENCOUNTERED THE TERM “ECOSYSTEM” in biology class. It refers, essentially, to any system of parts that are connected to and interact with one another. It’s actually a fairly modern notion, first introduced in 1935 by a scientist named A. G. Tansley.<sup>55</sup> He introduced the term as a sort of mashup of “ecology”—the relationship

between organisms and their environment—and “system”—a complex entity made up of interconnected parts. With the introduction of Tansley’s term, scientists suddenly had the means to describe something that had always existed but, nameless, hadn’t really been considered a topic worthy of study in its own right. Thanks to Tansley, people could look beyond two sets of things—individual creatures and the space in which they lived—and zoom out to a bigger picture, studying the interactions between creatures and their space.

This book is also in its way about creatures and space. There are two sets of creatures: the citizen-users of tech products and services; and net states, the makers and keepers of those products and services. Together, we traverse the same space—the digital. We and our interactions in the digital space generate our own kind of ecosystem: the digital ecosystem.

Ecosystems, in addition to having constituent parts, such as creatures and space, exhibit another important characteristic: they tend toward equilibrium, or a state of relative balance between opposing forces.<sup>56</sup> In nature, this means that enough creatures are born to offset the number who die; that enough nutrients are generated to replenish those that have been consumed.

For our digital ecosystem to be in a state of equilibrium, we—the creatures (both individual and net state) who inhabit the digital space—would have to get out as much as we put in. We citizen-users create content; we consume content. We upload photos, videos, and news; we download photos, videos, and news. These activities reflect what *looks* like a relatively steady state, but only if we disregard the net states that are our fellow ecosystem inhabitants.

With respect to our own content and net states, we’re *not* currently in a state of equilibrium. We’re not getting out as much as we’re putting in. Our content goes to net states, and then disappears behind their firewalls. We can’t see it all assembled. It goes into databases that generate insights—insights about our behaviors and habits and preferences—that net states gain benefits from but that we—the creators of the data—don’t necessarily know about and certainly don’t have access to.

This has to change. And we—the citizen-user content creators, the creatures who populate the digital ecosystem with our thoughts, our memories, our records, and our interactions—already have the power to ensure that it does change.

Without us, the digital ecosystem loses its life force. Websites absent of users interacting with them are virtual ghost towns, with no data to gather and analyze. We, the citizen-users, provide the energy that fuels the ecosystem; the net states provide only the space and pathways within it. So if we want our Declaration of Citizen-User Rights adopted, we have to use our power to withhold information from a website; to boycott usage; switch to a different service or platform that will agree to our terms and respect our rights. We can massively disrupt the equilibrium of the digital ecosystem, should we so desire. We just have to commit to doing it.

In short, it is in the best interests of all parties to the digital ecosystem to ensure that its human population is cared for. We don't need to deny ourselves the benefits that tech provides us. As *New York Times* "Smarter Living" editor Tim Herrera reflected, "When we talk about unplugging, I think what we're really talking about is structuring our lives in ways that allow technology to serve us, rather than the other way around."<sup>57</sup>

Right now, we serve tech companies—we give them our data, they generate insights based on that data, and we never see the results. We can continue to supply tech companies our data, but under different conditions—conditions, laid out in the Declaration of Citizen-User Rights, that give us control over and information about that data. We don't need to unplug and retreat from tech. We just need to adjust the equilibrium in the digital ecosystem.

AS OF 2017, THE WORLD HOSTED 65.6 MILLION PEOPLE WHO HAD BEEN forcibly displaced from their homes.<sup>58</sup> Refugees from war. Asylum seekers in search of protection because of their political or religious beliefs.

People displaced by their own countries, by their own compatriots. Ten million among them are considered officially “stateless” by the United Nations.<sup>59</sup> With these horrifying stats, the year 2017 ushered in a depressing new world record: an all-time high for displaced persons of every kind.

According to the US Department of State, a stateless person is defined as “someone who, under national laws, does not enjoy citizenship—the legal bond between a government and an individual—in any country.”<sup>60</sup> Notably, the definition contains the word “enjoy.” Citizenship in a country indeed offers something positive: It offers protections. It affords rights. While not all citizenships are created equal—the rights of citizens in the EU, for instance, are now quite different from those of citizens in the US—they do provide individuals with two invaluable benefits.

First, the fact of citizenship establishes a framework of expectations for what it means to be a contributing member of one’s society. For instance, most countries have some sort of legal document that details citizens’ rights and responsibilities in regard to the state, even if they’re as basic as freedom of speech and paying taxes. Second, citizenship, in democracies at least, grants rights that exist independent of who is in power. The president of the United States, for instance, may want to block someone on Twitter, as Donald Trump has expressed in many instances. But the Constitution, which protects freedom of speech, overrules that desire. According to court rulings, the president cannot block you or any other American citizen, because to do so violates the First Amendment, which guarantees freedom of speech. Citizenship in the United States means that you have power that outweighs the wishes of the (otherwise) most powerful person in the land—the president.<sup>61</sup>

In short, rights bring power. They are our protection against potential abuses of power. They are, according to the US Constitution, inviolate—something we’re born with as Americans. And we are fortunate to have rights. As Hannah Arendt, a philosopher who was stateless for 17 years, once wrote, “The right to have rights, or the right of every individual

to belong to humanity, should be guaranteed by humanity itself.”<sup>62</sup> She then added, “It is by no means certain whether this is possible.”

Net states, operating internationally, have the opportunity to afford their users rights that may differ from and even exceed rights of any individual’s nation-state (or, for the 10 million stateless, stand *in place* of citizenship rights). In this way, the rights afforded by net states rise above those guaranteed by nation-states.

The nation-state is no longer the only game in town. Nation-states can partner with net states, as we saw in the partnerships between Tesla and Vermont, California, and Connecticut. They can establish contracts with net states, as the federal government does in operating almost entirely on net state technology. Conversely, they can fight against net states: with regulations, as in the EU; with taxes, as in Uganda; or with bans, as in Papua New Guinea and Sri Lanka.

Whatever type of relationship nation-states and net states ultimately have, the reality is that there must be some sort of a relationship—and it must be diplomatic in nature, not just economic. As things now stand, net states don’t have just our information; they also have power over our rights. If nation-states don’t set the terms of how net states must operate with respect to our rights, then net states will write their own rules of engagement, in some cases avoiding regulations, as Facebook did when it moved more than a billion users out of its data center in Ireland—or adapting to them, as Google and Apple and Twitter have done to comply with the GDPR.

We—as citizens and citizen-users—have the right to have rights: with our nation-states and with our net states. It is up to our home countries to enforce the rights they’ve granted in our constitutions. And it is up to us as individuals to hold our net states accountable if they fail to grant us protection with respect to those rights. The US Constitution holds that we have the right to “be secure in [our] persons, houses, papers, and effects.” Our data may not be who we are, but it is certainly something of us. As such, it is something that needs to be secured.

TUCKED AWAY IN THE CORNER OF THE FIRST FLOOR OF THE UNITED Nations General Assembly building—that low, white, asymmetrical building with a dome atop and 192 country flags in front—sits a tiny, inconspicuous, triangular room. It’s virtually empty. It has a few rows of benches in the back, an abstract cubist-style mural at the front. In the center stands a six-and-half-ton rectangular block of polished iron ore, perennially cool to the touch. It’s illuminated by a single beam of light. This is the so-called meditation room.

The second secretary-general of the United Nations—the everyman’s aristocrat, the sky-eyed Swede, Dag Hammarskjöld, who’s widely regarded as a founding architect of the organization itself—personally redesigned the space in 1957. The original setup in 1952 was a dreary place, with tightly packed rows of chairs facing what looked like a tree stump holding up a flower arrangement and a tired-looking miniature UN flag.<sup>63</sup> Aesthetically, the room didn’t inspire serene thoughts; it looked more like a shrunken, misshapen conference room.

According to a reporter working at the UN at the time, in the middle of one night in 1956, Hammarskjöld, still at work, dragged some of his aides out of their offices. Having been summoned by the secretary-general himself in the wee hours of the morning, they expected to be told bad news from one of the far-off war zones where United Nations personnel were on the ground. Instead, he said, “I want to go down to the meditation room.” Because this was the secretary-general himself making this request, they followed—even at two in the morning.

Hammarskjöld wanted to talk to them about the utmost importance of redesigning this room. “We want to bring back, in this room, the stillness which we have lost in our streets, and in our conference rooms,” he told his aides, “and to bring it back in a setting in which no noise would impinge on our imagination.” In the subsequent year, Hammarskjöld took on the meditation room as a personal project, dictating details ranging from the color of the paint on the walls to the fabric of the carpet.<sup>64</sup> In his formal dedication of the room in 1957, four years before he would be killed in a plane crash in the Congo, he called attention to the

iron stone altar in particular, asking visitors to ask themselves: What they would make out of iron, such a powerful material—would they use it to craft the means to support war or to sustain life?<sup>65</sup>

He wrote, “Of iron he has constructed tanks, but of iron he has likewise built homes for man. The block of iron ore is part of the wealth we have inherited on this Earth of ours. How are we to use it?”

The meditation room, like most rooms, has a practical function. It’s a place to meditate, to reflect. But its real significance is symbolic. This place is something that one of the founding fathers of the United Nations obsessed over getting right. And it’s not like he had nothing else to occupy his time: Hammarskjöld, in his tenure as secretary-general, was responsible for onboarding 4,000 new UN staffers and establishing how they’d work and what’d they’d do. And he had a nightmare’s worth of thorny diplomatic demands: trying to establish peaceful relations between Israel and the Arab states; negotiating the release of captured US pilots during the Korean War; untangling the Suez Canal crisis; establishing the United Nations Emergency Force, the first-ever officially sanctioned nationless military unit; and attempting to orchestrate the decolonization of the African continent.

Hammarskjöld cared about the meditation room because of what it represented. It would serve as a reminder to every king, queen, president, and prime minister who would someday walk the halls of the United Nations building that they should, at some point, stop to meditate. Stop to think. To wonder: Is this work I do creating a better world? Am I taking the resources at my disposal—the iron ore of my era—and molding it into opportunities for my people? Or am I just making tools that will bring about their destruction?

## CONCLUSION



# THE NET STATE PATTERN

**H**ello? Uh, hello? Hello, Dmitri? Listen, I can't hear too well; do you suppose you could turn the music down just a little? Aha, that's much better," begins the phone conversation between two fictional world leaders, the American president Merkin Muffley and the Soviet premier Dmitri Kissov, in Stanley Kubrick's 1964 classic film *Dr. Strangelove, or: How I Learned to Stop Worrying and Love the Bomb*.

"Now then, Dmitri," says the US president, "you know how we've always talked about the possibility of something going wrong with the bomb." Pause. "The *bomb*, Dmitri. The hydrogen bomb." He continues, "Well now, what happened is, uh, one of our base commanders, he had a sort of—well, he went a little funny in the head. You know. Just a little funny. And uh, he went and did a silly thing." The president sighs. "Well, I'll tell you what he did. He ordered his planes . . . to attack your country."

In the absurd exchange that follows, the US president tries to talk his Soviet counterpart off the ledge, assuring him that this was all just a big misunderstanding and that he was really sorry and they'd figure out some way to deal with it. The scene captured both the frightfully high

stakes and the fragility of relations between the United States and the Soviets in the 1960s. The exchange also employed a piece of technology absent in the actual diplomatic communication channels between the two nuclear powers: a dedicated and secure telephone system that linked the two powers.

The satirical film captured the mood of the era in part because of how closely it mirrored reality. Just two years prior, the world had held its breath watching the Cuban missile crisis play out. This 13-day stand-off in which the United States and the Soviet Union debated whether to blow each other and the world to smithereens in a nuclear war was, in part, elevated due to faulty communication channels between the two countries.

On October 24, 1962, at 6 p.m., Soviet premier Nikita Khrushchev messaged a fierce 3,000-word missive to the Americans, declaring that “the actions of the United States with regard to Cuba constitute outright banditry or, if you like, the folly of degenerate imperialism.” He spelled out the stakes in no uncertain terms, saying, “Unfortunately, such folly can bring grave suffering to the peoples of all countries, and to no lesser degree to the American people themselves.” Khrushchev then directly threatened war: “The Soviet government considers that the violation of the freedom to use international waters and international air space is an act of aggression which pushes mankind toward the abyss of a world nuclear-missile war.”<sup>1</sup>

Diplomacy is generally a careful affair, in which participants deploy measured language; threats are typically inferred from a combination of painstaking reading-between-the-lines and outright guesswork. Compared to the norm, Khrushchev’s letter was about as subtle as a bazooka blast across the bow.

But it was a blast that took an obscene amount of time to register with the Americans. They didn’t get the letter decoded and translated until 11 a.m. the next day—almost 12 hours after the Soviets sent it. Given the stakes—mutually assured destruction—and the intensity of Khrushchev’s letter, it must have seemed baffling to the Soviets that

they didn't receive some sort of response from the US during that initial half day. So while the Americans were scrambling to decode and translate the original letter, the Soviets sent another, even more bellicose letter. The situation quickly elevated from verbal trash talk of war to the actual, imminent risk of it.

While many interceding twists and turns ensued, for the purposes of this discussion I will skip to the end: in a massive diplomatic gamble, the Americans decided to simply claim they had never received the second letter.<sup>2</sup> By essentially pretending it had gotten lost in the mail, the Americans and the Soviets were both able to blame poor communication for this diplomatic nightmare, save a modicum of face, and, lock-eyed with one another at every step, back away from the brink of nuclear war.<sup>3</sup>

With nuclear annihilation averted, both sides vowed to never again let convoluted communication channels stand in the way of avoiding Armageddon. They turned to technology for an answer. The Washington-Moscow hotline was born.

Despite Hollywood depictions of a red telephone, the hotline was actually a clunky teletype machine that routed signals from Washington through a series of relays—via London, Copenhagen, Stockholm, and Helsinki—before they reached Moscow. As we've seen, undersea cables are vulnerable to physical damage, and the cable involved in this linkup was no exception—it was accidentally severed several times, including by a bulldozer in Copenhagen and by a Finnish farmer who inadvertently snagged it while plowing.<sup>4</sup>

Further complicating communication via that particular means, the teletype used wasn't just a machine, but a set of them—one was a backup in case the first failed—each equipped with English and Cyrillic keypads. They were tested on an hourly basis every day since being installed over fifty years ago, on August 30, 1963.<sup>5</sup> The technology's been upgraded since then—we've moved on from teletype to encrypted email by now—but the dedicated communications channel and testing protocols have remain unchanged for over half a century.

The very first test was almost a diplomatic disaster in itself. To ensure that all the keys worked, the inaugural test from the United States consisted of the sentence, “The quick brown fox jumped over the lazy dogs”—words that any keyboard user would recognize as a standard test sentence, used because it contains all the letters of the English alphabet. Puzzled at the message, the Soviets on the receiving end inquired as to its meaning. The Americans quickly clarified that this was a standard keyboard test and *not* some cryptic code. The Soviets then replied with their own surprisingly humanizing test message: a lyrical description of a Moscow sunset.

Technology has transformed the *way* we communicate with our global partners. But it cannot replace the guts of *how* we communicate—the need to understand foreign languages, cultures, and the context affecting one’s counterparts.

Even among people with similar backgrounds—say, Silicon Valley entrepreneurs—there’s only so much communication that technology can effectively convey. As physical creatures, we still assess one another through nonverbal cues—physical appearance, body language, style of dress, posture, tone, volume, and so on. In a seminal study of thousands of interviews and negotiations, researchers determined that body language accounts for upwards of 60 to 80 percent of the impact made around a negotiating table.<sup>6</sup> Furthermore, people establish 60 to 80 percent of their initial opinions about their conversation partners within the first four minutes of their interaction. The words we say matter, but how we say them and who people perceive us to be may matter even more.

As legendary journalist Edward R. Murrow put it, “The really critical link in the international communications chain is the last three feet, which is best bridged by personal contact—one person talking to another.”<sup>7</sup> This applies to any communication chain, really, not just diplomatic ones.

And we’re beginning to see net states take this concept to heart. As they begin to coordinate efforts around defense and diplomacy on their

platforms and services, despite being armed with the most sophisticated communication tools on the planet, Facebook and Google and Amazon and the like are finding ways to bridge the last three feet. They're convening in person.

FACEBOOK, WHILE ITS FOUNDERS MAY NOT HAVE FORESEEN THIS BACK in Zuckerberg's dorm room days, has evolved beyond just social networking. Its people and tools are fighting extremists, as we saw in chapter 4. What's more, in 2018 Facebook increased the size of its internal counterterrorism team by over 30 percent.<sup>8</sup> With approximately 200 staffers solely devoted to counterterrorism, this unit is still only a minuscule portion of Facebook's total workforce of over 25,000 employees. But its growth rate—from unit launch in 2016 to a force 200 strong in just two years—signifies that this is a trend that's unlikely to reverse anytime soon.<sup>9</sup>

Monitoring for offensive or illegal activity, like it or not, occupies a lot of Facebook's energy these days. It's not alone among net states in this, and it's not going it alone either. It's teaming up with its kin. On December 5, 2016, Facebook, Microsoft, Twitter, and YouTube (Google) announced a partnership to stem the spread of online terrorist content.<sup>10</sup> Six months later, the same foursome announced the formation of the Global Internet Forum to Counter Terrorism, a partnership intended to create information-sharing channels between the participants to better combat terrorism using their products.<sup>11</sup>

Whether those initiatives generated any significant results is difficult to discern; the tech companies have released few details publicly since their initial announcement. But what we do know is that there's a noticeably absent player in these partnerships: government.

To be fair, the firms tried reaching out to government, once. On May 23, 2018, about a year after their initial convening, Facebook assembled representatives from Amazon, Apple, Google, Microsoft, Oath (a major ad agency for net states), Snap (high-end tech consultants), and Twitter.

It also invited representatives from the US Department of Homeland Security and the FBI. The agenda: to talk about how to prepare for foreign attempts to influence the 2018 midterm elections.<sup>12</sup>

The meeting was a disaster. To put it politely, the event was “tense,” according to a participant who did not wish to be named. After sharing privileged information with the US security apparatus, the net states got little in return other than tight-lipped “no comment” responses from their government counterparts. The tech firms left the meeting discouraged. According to one person present, “the encounter led the tech companies to believe they would be on their own to counter election interference.”

Just a few months later, on August 23, 2018, a dozen major tech companies held another meeting on the same topic, hosted by Twitter.<sup>13</sup>

This time, they didn’t bother to invite government.

WHETHER NET STATES ARE INDEED ON THEIR OWN IN FIGHTING FOREIGN infiltration of their platforms or not, they believe that they are. Indeed, they may be better equipped for that fight than is government. In an off-the-record conversation in the spring of 2018, a senior FBI official told me, “The truth is, we need them much more than they need us.” When I asked why that was, he said they couldn’t hire enough staff with expertise at the intersection of tech and terrorism: federal agencies pay a pittance compared with tech companies. “We’re just not competitive.”

This isn’t a good sign for you, government. I write this as a believer in the power of government; indeed, as a government official myself. If officials don’t work with net states, these firms will only expand further into territory that used to be government’s primary dominion. If government tells net states that they’re on their own in the fight against non-state-sponsored terrorist activities online, and that they’ll also have to deal with state-sponsored cyberattacks from Iran, Russia, and other countries alone, they most certainly will do it; and—unhampered by the need to comply with laws and regulations—they’ll likely do it well.

Without government assistance, net states have no choice but to deal with these issues on their own: terrorism on their platforms is an existential threat. Because if net states allow their ecosystem to be polluted by terrorists and by Russian and Iranian (and other) misinformation warfare campaigns, regular users may very well take their profiles and their data and, worse, their attention elsewhere.

My recommendation for government is this: engage. It's not too late to partner with net states. Appoint your own tech ambassadors. Set up diplomatic channels to net state leadership. Because there isn't much time left; the window to net state decision-makers will at some point close. Net states are already taking action in defense and diplomacy without government—no, *above* government. They are already investing in public infrastructure, which they will then possess slices of ownership over. They already manufacture the physical devices stowed in the vast majority of Americans' pockets: our phones. They already supply the platforms and services that ferry the content of a vast majority of Americans' thoughts. In short, net states are already gaining ground into defense, diplomacy, public infrastructure, citizen services, and even food services. And they're likely to only gain more ground in these areas as time goes on.

Nation-states—and government generally—will become increasingly irrelevant if they continue to cede power to net states, especially if they do so as a byproduct of inattention. And inattention is what appears to be driving these policies of noncooperation. It's highly doubtful that the Department of Homeland Security and the FBI have any clearly defined policy that stipulates intentional nonpartnership with technology companies. Being a government official, I've seen how policy often gets made: by adopting whatever the default is—by not actually *having* a policy. The default becomes the norm, the norm slides into the expected, and the expected eventually gets cemented as the official. Thoughtful and considered reflection is all too often absent in the process. Especially when it comes to confronting new and not-well-understood tech, government's default response is pretty much always no.

The competence with which net states are filling the leadership void left by the government's default policy could be the wake-up call nation-states need to recognize just how powerful net states have become. Conversely, it could lead to the systemic unraveling of the nation-state system as we know it.

In "The Demise of the Nation State," an article the British Indian novelist Rana Dasgupta wrote for *The Guardian*, he suggests that this wouldn't be such a bad thing.<sup>14</sup> He points to how the nation-state system counters the notion of universal human rights.

"Citizenship," he writes, "is itself the primordial kind of injustice in the world. It functions as an extreme form of inherited property and, like other systems in which inherited privilege is overwhelmingly determinant, it arouses little allegiance in those who inherit nothing." In other words, if you're lucky enough to be born in the United States or Sweden or the UK, you automatically "inherit" a better quality of life than if you happen to be born in Somalia or North Korea, whose governments are either too weak or too dictatorial to protect human rights.

Alex Tabarrok makes a similar case in his 2015 article for *The Atlantic*: "The Case for Getting Rid of Borders—Completely."<sup>15</sup> He contends that, "no standard moral framework . . . regards people from foreign lands as less entitled to exercise their rights—or as inherently possessing less moral worth—than people lucky to have been born in the right place at the right time."

There are plenty of others also making similar arguments: advocating for, predicting, or otherwise presaging the beginning of the end of the nation-state system. I don't think we're there yet. But unless the US government takes up the mantle of responsibility set forth in the Constitution—to "promote the general welfare" and "secure the blessings of liberty to ourselves and our posterity"—it will miss its chance to influence how the international order is going to shake out in the coming decades.

“TYRANNY” IS GENERALLY DEFINED AS SOME VERSION OF “OPPRESSIVE power.” It’s been a loaded word in America since the beginning. The founding fathers were particularly fond of the term. Thomas Jefferson used it liberally in his writings, citing “tyrannical” rule from the United Kingdom twice in the Declaration of Independence. He wrote, in a letter to a colleague in the fight for independence, “I have sworn upon the altar of god eternal hostility against every form of tyranny over the mind of man”—words so emblematic of his philosophy that they’re engraved on the Jefferson Memorial in Washington, DC.<sup>16</sup> James Madison, attempting to reassure the American people that the Constitution would protect against tyranny, specifically addressed that matter in the Federalist Papers (no. 46). If every country had the separation of powers that’s set out in the American Constitution, he said, “the throne of every tyranny in Europe would be speedily overturned.”<sup>17</sup> The Second Amendment of the Constitution, dealing with the right to bear arms, was born out of the framers’ concern over the possibility of tyrannical rule; it ensured that the citizenry would have the ability to rise up against such forces.<sup>18</sup> Of course, that was then; today, there’s virtually no chance that even if you armed every man, woman, and child in the United States we could defeat the steamroller that is the US military apparatus. But the anti-tyranny argument is still a popular one in gun law debates.

This is important background to keep in mind when considering why the government doesn’t do more to protect us against potentially damaging net state practices. We as a citizenry grew into our present state with a deep distrust of government. This is one of the reasons for the establishment of the federal system of separating powers.

“If men were angels, no government would be necessary,” as James Madison put it in the Federalist Papers (no. 51), going on to write that “in framing a government which is to be administered by men over men, the great difficulty is this: You must first enable the government to control the governed; and in the next place, oblige it to control itself.”<sup>19</sup>

So, controlling itself—through the system of checks and balances—is embedded in the foundation of our government. While the American

system didn't come out of thin air—ancient Rome was governed through a separation of powers, and such governance was popular in the writings of a number of influential political philosophers, including Baron de Montesquieu and John Locke—in modern history, the United States was among the first nations to implement the system.<sup>20</sup> In so doing, the US established checks and balances as a hallmark of the modern democratic state that would go on to be adopted by countries the world over.

True to our roots, we persist in our distrust of government. As discussed in chapter 6, Americans seem to accept that net states and marketing firms and data brokers will compile profiles on us in incredible detail. However, we will simply not tolerate the idea that *government*—that entity capable of “tyranny,” in the popular imagination—might have anything more than the most basic data about us. When National Security Agency contractor Edward Snowden leaked to the public information about the metadata collection program PRISM in 2013, Americans freaked out, as we saw earlier. The fact that it was only metadata that was collected, and that metadata contains only information *about* communications, not the *content* of communications—not what person X said to person Y—got lost in most of the public discourse surrounding PRISM. The Snowden leaks, as they've come to be known, led Americans to become even more distrustful of how their government handles people's private information. In one poll, 70 percent of respondents reported that they believed the government used the data collected in that program “for purposes beyond anti-terror efforts.”<sup>21</sup>

We didn't trust government when we formed as a nation. We don't trust it now. Actually, we don't trust much, when you really get down to it. Owing in part to a toxic partisan political climate following the 2016 presidential election, Americans in early 2018 reported feeling a loss of trust in one another, in the media, in institutions of government, in tech companies—in just about every index measured on a global “Trust Barometer,” with trust dropping 23 points from the previous year, placing the US at 18th out of 26 countries surveyed.<sup>22</sup>

But there's an important distinction to be made between our report-

ing a loss of trust in government and a loss of trust in net states. We *need* our government in order to live safe, orderly lives. As we have seen, government is charged to provide the foundation that permits exactly that; it is to “establish justice,” “insure domestic tranquility,” “promote the general welfare,” and “secure the blessings of liberty.”

We don’t *need* our net states in the same way. Or do we? Do we need them in order to live safe, orderly lives? Will they work toward justice, tranquility, our general welfare, and our blessings of liberty?

Increasingly, it seems that they may. They’re rooting out terrorists on their platforms. They’re shutting down accounts promoting hateful rhetoric. They’re issuing diplomatic statements condemning practices that violate fundamental human rights. They’re giving us tools that shoo us *off* their tools. They are, in their own way, looking out for us—as citizen-users. It may have nothing to do with principles: what’s “right” or what’s “just.” It may have everything to do with protecting their ecosystem; preserving their own health and the health of us as the creatures who coinhabit it. Regardless of the motivations, genuinely protective action on the part of net states appears to be happening. The question remains, though, Can we expect it to *keep* happening? Can we ask for even more of it? And how?

And finally, the question for us to ask ourselves—you and me and everyone we know—is, What to do about government? If we need government—and we would be literally lawless and defenseless without it—how can we rebuild our trust in it; get it fully functioning, to where citizens participate in affairs of the state and feel powerful for their participation?

One last set of quotes from James Madison. He argued, “If Tyranny and Oppression come to this land, it will be in the guise of fighting a foreign enemy.”<sup>23</sup> In a 1798 letter to Thomas Jefferson, he wrote, “It is a universal truth that the loss of liberty at home is to be charged to the provisions against danger, real or pretended, from abroad.”<sup>24</sup>

We as a citizenry are indeed fighting foreign enemies—from non-state actors to nation-state actors. We have been fighting foreign enemies

in the current war on radical Islamist terror for 18 years, with no end in sight. And we know war well: the United States has been at war for 148 years out of our 243-year existence—and that’s excluding the 45-year-long Cold War, our decades-long hostilities with Iran and North Korea, and our relationship with countries that conduct cyberattacks against American infrastructure, media, and our financial industry<sup>25</sup> on a regular basis.

Net states know us to a degree; as individuals, as a people. But they’re not *responsible* for us; they are not responsible for our defense and they are not responsible for our well-being. *Government* is. And it’s ours, as Roosevelt said: “We are the government—you and I.” We face too many foreign enemies to ignore how much we need government to defend us. And we face too many domestic injustices to ignore how much we need government to serve us.

As we search—for information, for advice, for ways to better our days—we must remember to also search deeper: for meaning, for purpose, for something greater than ourselves. We can help ourselves as individuals and as a citizenry by searching for ways to see ourselves more clearly. And we can work with those who wield power over us—our net states and our nation-state—to protect and defend us from enemies foreign and domestic; from our own worst habits; and in pursuit of our better selves.

ON THE OUTSIDE, METEORITES LOOK MUCH LIKE ORDINARY EARTH rocks. Indeed, earth rocks and space rocks appear virtually indistinguishable. But if you split open a meteorite and etch it with weak acid, a pattern emerges. This pattern is called the Widmanstätten pattern. It doesn’t occur in any rock on earth.

The pattern looks like a series of geometric cross-hatching, technically described as a “three-dimensional octahedral structure.”<sup>26</sup> While the pattern can be reproduced on earth rocks, it doesn’t last; its lines distort over time.<sup>27</sup> In the end, the pattern is wholly unique to mete-

orites. It takes a little work to see it; you have to look past the surface layer, apply a little technique. But once you do the work, the pattern is unmistakable.

Net states are not so different. They look like ordinary companies, just as earth rocks look like meteorites. They are not nation-states, though they increasingly engage in activities that nation-states usually handle. Net states are something unique. And they too have their tell-tale marks, their Widmanstätten pattern. Net states are tech companies, with a cause. They are tech collectives, with an agenda. They are tech believers, loosely unified. They possess physical resources, political means, and social capital. They are of countries, and beyond them. They are in virtually every aspect of our lives, yet for the most part effectively invisible to us.

We may occasionally wish we could go back to a time when we had control of all our data—when we didn't have to worry that the foolish pictures we took in college would end up on someone's Facebook page, when that professional embarrassment didn't end up being so easy to find on Google. But there's no unringing this bell. Net states are here to stay.

The best we can do is become knowledgeable about how they operate, why they do what they do, and what their underlying agendas are—beyond the obvious one: money. Also, we owe it to ourselves to figure out how to protect our data and our identities while still remaining productive members of the digital ecosystem. We must become the technological version of armchair geologists, able to identify a net state from a regular old tech company or flash-in-the-pan online movement. We must be able to spot their Widmanstätten pattern and, once we do, pay a very particular kind of attention to them.

This book is one of the first attempts I know of to chronicle the existence of net states and analyze how they impact our lives. But the specific examples in this book aren't really the point. Net states adapt, change, evolve, or perish. Whether we're talking about Google or Facebook or a net state that won't launch until tomorrow or a net state that

dies before this book goes to print is almost irrelevant. What matters is that we keep the *pattern* of net states in mind: they are of the tech ethos; they advance belief-driven agendas; and they are international in scale and scope. And we empower them each time we use their devices, platforms, and services; we control their fate with every click, keystroke, and swipe.

We have to make those actions matter: they add up, especially with so many of us using the internet. With net states, our habits are our votes. And the more we understand the pattern of what net states are and how much of our data they have, how deeply into our lives they reach, the more likely we will be able to mobilize like-minded others to push back.

It may feel like too much to expect. Who are we, after all, as individual citizen-users, to demand that multibillion-dollar tech companies change their ways? As individuals, we may not have much clout. But tech itself has given us the ability to mobilize in ways never before possible.

As the novelist Alice Walker once said, “The most common way people give up their power is by thinking they don’t have any.”<sup>28</sup> Every single tech user has power over their net states. We just have to claim it.

## ACKNOWLEDGMENTS

There's a story behind this book. I didn't start out thinking I would write one. My original plan was just to get an article published, for which I have Joanna Pearlstein at *WIRED* to thank. It came out in November 2017 and caught the attention of NPR's *Science Friday* program. I thank Ira Flatow, who invited me to appear on air alongside the whip-smart tech journalist Max Reed, for the chance to bring my ideas to the airwaves.

Because it was after that segment that things suddenly started happening: Roger Freet, my esteemed literary agent at Foundry Media, was driving to the package store when my episode of *Science Friday* aired. He said he was listening to the radio, heard my description of net states, and pulled over to take out a pen and write down my name. He found my email address online and reached out with what really is one of the best questions in the world: Would I be interested in turning this idea into a book?

Roger coached me through the grueling process of converting a 700-word article into a proper full-length book proposal with incredible patience, generosity of spirit, and plain old blind faith. I am enormously grateful for his encouragement and support, and for guiding the book to its publishing home at HarperOne, with my superstar editor, Miles Doyle.

I happen to know a little bit about editors, having the great good fortune of being married to one of the most successful editors in the

business, Jonathan Tepperman (more on him later). One of the best descriptions of Miles's contribution to this book came from my husband. Upon reading my final draft, Jonathan said, "I don't know exactly what Miles did, but you should be extremely happy to have him on your side—this version is light years better than the first draft I read!" It is indeed, and I owe a massive thanks to Miles for his insightful, thoughtful, and always-encouraging approach to editing this book. I am also deeply indebted to Kathy Reigstad for her surgical-precision copyediting, which transformed this from manuscript to proper book, ready for the world.

I wrote this book while also working a full-time job as press secretary at the New York City Department of Veterans' Services, taking every Sunday from 4 a.m. to noon to write, and squishing in writing during odd hours each week with my boss's encouragement. My boss, Loree Sutton, MD, Commissioner, Brigadier General (ret.), US Army, is a boss people dream of. I couldn't have written this book without her encouragement, support, and flexibility, as well as the professionalism and camaraderie of all my incredible colleagues, especially Jeffrey Roth, Ellen Greeley, Cassandra Alvarez, Jason Parker, Eric Henry, Aquilla Hines, Venkat Motupalli, and, above all, my counterpart, Gabriel Ramos.

In addition to being a government official, I am blessed to be able to teach part-time at Columbia University's School of International and Public Affairs (SIPA). I am eternally grateful for and owe enormous thanks to Anya Schiffrin, Dan McIntyre, and Merit Janow for the chance to be a part of the SIPA family.

It was through SIPA that I met my intrepid research assistant, CJ Dixon, whose discoveries opened my eyes to possibilities I would never have found without him. I also owe a huge debt of gratitude to my "Technology, National Security, and the Citizen" students, whose fascinating insights informed so many topics in this book—with a special thanks to my teaching assistant, Camilia Razavi.

Those who lent me the brainpower, moral support, and wisdom that lifted this book to a whole new level deserve special praise, as they

had to wade through my less-than-polished ideas and drafts. Their insights made the book a far better final product, and I am lucky to have them on my side: Alexandra Farkas, Aliya Bhatia, Aquilla Hines, Camilia Razavi, Chet Wichowski, Christine Cearnal, Dahna Black, Danielle Tomson, Dawn Emsellem, Emily Boitel, Gabriel Ramos, Jacqueline Burns Koven, Joel Putnam, Katherine Garcia, Keith Wichowski, Madison Jacox, Marijka Hoczko, Matthew Burton, Michael McColpin, Natasha Cohen, Shalaka Jokshi and Venkat Motupalli—thanks for being so incredibly generous with your time and mental energy.

As a parent of school-age children, I couldn't do any work at all without a team of responsible, committed caregivers. A huge, heartfelt thank-you to Chanise Martineau for ensuring that my littlest remained happy, safe, and loved while I worked; and my most sincere appreciation for all the dedicated teachers at Congregation Beth Elohim, MS 51, and Williamsburg Prep, who make my children smarter, kinder, and better people by the day.

My family. It gives me tremendous pleasure to recognize them, my inner orbit, the people who most inspire and sustain me: my parents, Chet Wichowski and Marijka Hoczko; my brother and team, Keith Wichowski, Dawn Emsellem, Milo, Andre, and Desi; my Canadian family, the Teppermans—Bill and Rochelle; Noah, Julie, Lily, and Benji; Andrew, Tina, Lia, and Nathan; and my dear and lifelong friends, Christine Cearnal and Alexandra Farkas.

Of course, I would be nothing without my nucleus: my children, Gerome, Novi, and Leo, and my husband, Jonathan. Gerome, Novi, and Leo, watching you grow and guiding your progress into the wonderful human beings you are is the greatest thing I've ever been a part of, and I'm so grateful I get to care for you and just plain delight in you.

Jonathan, being in your presence makes me want to be the best version of myself. I would not have been able to write this book without you—literally, as it was only because you were willing to watch our four-year-old single-handedly every Sunday for a year (a year!) that I had time to write, and in every other possible sense as well. I'm inspired

by you; I'm awed by you. I am so very grateful for you. Thank you for being you. Thank you for choosing me.

# APPENDIX

| CATEGORY                    | NAME                          | SUBSIDIARY OF | INVESTED IN BY | ACQUIRED BY |
|-----------------------------|-------------------------------|---------------|----------------|-------------|
| Agriculture & food services | Farmers Business Network      |               | Google         |             |
| Agriculture & food services | The Climate Corporation       |               | Google         |             |
| Agriculture & food services | Granular                      |               | Google         |             |
| Agriculture & food services | Bowery Farming, Inc.          |               | Google         |             |
| Agriculture & food services | Abundant Robotics             |               | Google         |             |
| Agriculture & food services | Solum                         |               | Google         |             |
| Agriculture & food services | Impossible Foods              |               | Google         |             |
| Agriculture & food services | LevelUp                       |               | Google         |             |
| Agriculture & food services | Soylent                       |               | Google         |             |
| Agriculture & food services | Juicero                       |               | Google         |             |
| Agriculture & food services | Ripple Foods                  |               | Google         |             |
| Agriculture & food services | Clear Labs                    |               | Google         |             |
| Agriculture & food services | Siddhivinayak Agri Processing |               | Google         |             |
| Agriculture & food services | Whole Foods Market            |               |                | Amazon      |
| Agriculture & food services | Ocean's Halo                  |               | Facebook       |             |
| Agriculture & food services | Rise                          |               | Google         |             |
| Biotech                     | Evelo Biosciences             |               | Google         |             |
| Biotech                     | BenchSci                      |               | Google         |             |
| Biotech                     | ARMO BioSciences              |               | Google         |             |
| Biotech                     | Magenta Therapeutics          |               | Google         |             |
| Biotech                     | 23andMe                       |               | Google         |             |
| Biotech                     | Arcus Biosciences             |               | Google         |             |

| CATEGORY          | NAME                       | SUBSIDIARY OF | INVESTED IN BY | ACQUIRED BY |
|-------------------|----------------------------|---------------|----------------|-------------|
| Biotech           | FLX Bio                    |               | Google         |             |
| Biotech           | Forty Seven                |               | Google         |             |
| Biotech           | IDEAYA Biosciences         |               | Google         |             |
| Biotech           | SQZ Biotech                |               | Google         |             |
| Biotech           | BlackThorn Therapeutics    |               | Google         |             |
| Biotech           | GLO                        |               | Google         |             |
| Biotech           | XtalPi                     |               | Google         |             |
| Biotech           | Gritstone Oncology         |               | Google         |             |
| Biotech           | Vaccitech                  |               | Google         |             |
| Biotech           | Cala Health                |               | Google         |             |
| Biotech           | Arsanis                    |               | Google         |             |
| Biotech           | Alector                    |               | Google         |             |
| Biotech           | Obsidian Therapeutics      |               | Google         |             |
| Biotech           | Fulcrum Therapeutics       |               | Google         |             |
| Biotech           | Cambridge Epigenetix       |               | Google         |             |
| Biotech           | iPierian                   |               | Google         |             |
| Biotech           | Adimab                     |               | Google         |             |
| Biotech           | Genomics Medicine Ireland  |               | Google         |             |
| Biotech           | SynapDx                    |               | Google         |             |
| Biotech           | Transcriptic               |               | Google         |             |
| Biotech           | SpyBiotech                 |               | Google         |             |
| Biotech           | NeuroVigil                 |               |                | Elon Musk   |
| Biotech           | DNAexus                    |               | Microsoft      |             |
| Biotech           | Rosetta Biosoftware        |               |                | Microsoft   |
| Drones & delivery | GoJek                      |               | Google         |             |
| Drones & delivery | EasyPost                   |               | Google         |             |
| Drones & delivery | Sidecar Technologies       |               | Google         |             |
| Drones & delivery | Convoy                     |               |                | Amazon      |
| Drones & delivery | Airware                    |               | Google         |             |
| Drones & delivery | Skycatch                   |               | Google         |             |
| Drones & delivery | Cape Productions           |               | Google         |             |
| Drones & delivery | Hivemapper                 |               | Google         |             |
| Drones & delivery | Ascenta (UK)               |               |                | Facebook    |
| Energy            | SolarCity                  |               | Google         |             |
| Energy            | Transphorm Inc.            |               | Google         |             |
| Energy            | Cool Planet Energy Systems |               | Google         |             |

| CATEGORY    | NAME                          | SUBSIDIARY OF | INVESTED IN BY | ACQUIRED BY |
|-------------|-------------------------------|---------------|----------------|-------------|
| Energy      | EDF Renewable Energy          |               | Google         |             |
| Energy      | BrightSource Energy           |               | Google         |             |
| Energy      | Clean Power Finance           |               | Google         |             |
| Energy      | Alta Wind Energy Center       |               | Google         |             |
| Energy      | Makani Power                  |               | Google         |             |
| Energy      | Center for Resource Solutions |               | Google         |             |
| Energy      | Makani Power                  |               |                | Google      |
| Energy      | Outride                       |               |                | Google      |
| Energy      | SolarCity                     |               |                | Tesla       |
| Energy      | Zep Solar                     |               |                | SolarCity   |
| Energy      | Paramount Solar               |               |                | SolarCity   |
| Energy      | Off Grid Electric             |               | Tesla          |             |
| Energy      | Valence Technology            |               |                | Microsoft   |
| Energy      | Silevo                        | Tesla         |                | SolarCity   |
| Energy      | Iliosson                      |               |                | SolarCity   |
| Energy      | Palo Alto Solar               |               |                | SolarCity   |
| Energy      | Declination Solar             |               |                | SolarCity   |
| Energy      | BuffaloGrid                   |               | Microsoft      |             |
| Energy      | Xively                        |               |                | Google      |
| Environment | Gradient                      |               | Google         |             |
| Geopolitics | Jigsaw                        | Google        |                |             |
| Geospatial  | echoecho                      |               | Google         |             |
| Geospatial  | Keyhole Inc.                  |               |                | Google      |
| Geospatial  | indoor.io                     |               |                | Apple       |
| Geospatial  | BroadMap                      |               |                | Apple       |
| Geospatial  | Locationary                   |               |                | Apple       |
| Geospatial  | WifiSlam                      |               |                | Apple       |
| Geospatial  | FlybyMedia                    |               |                | Apple       |
| Geospatial  | Color Labs Inc.               |               |                | Apple       |
| Geospatial  | Poly9                         |               |                | Apple       |
| Geospatial  | MapSense                      |               |                | Apple       |
| Geospatial  | Coherent Navigation           |               |                | Apple       |
| Geospatial  | Glancee                       |               |                | Facebook    |
| Geospatial  | MultiMap                      |               |                | Microsoft   |
| Geospatial  | Spindle                       |               |                | Twitter     |

| CATEGORY          | NAME                    | SUBSIDIARY OF | INVESTED IN BY | ACQUIRED BY |
|-------------------|-------------------------|---------------|----------------|-------------|
| Government        | Vicinity                |               |                | Microsoft   |
| Government        | Fast Search & Transfer  |               |                | Microsoft   |
| Health & wellness | ClassPass               |               | Google         |             |
| Health & wellness | ProtoGeo Oy             |               |                | Facebook    |
| Health & wellness | Bedditt                 |               |                | Apple       |
| Health & wellness | Glimpse                 |               |                | Apple       |
| Health & wellness | Hello Heart             |               | Facebook       |             |
| Health & wellness | Fight The Stroke        |               | Microsoft      |             |
| Health & wellness | MD.Voice                |               | Microsoft      |             |
| Health & wellness | Mgv                     |               | Microsoft      |             |
| Health & wellness | Medstory                |               |                | Microsoft   |
| Health & wellness | Global Care Solutions   |               |                | Microsoft   |
| Health & wellness | Sentillion              |               |                | Microsoft   |
| Health & wellness | Flatiron Health         |               | Google         |             |
| Health & wellness | Clover Health           |               | Google         |             |
| Health & wellness | Quartet                 |               | Google         |             |
| Health & wellness | Collective Health       |               | Google         |             |
| Health & wellness | One Medical             |               | Google         |             |
| Health & wellness | Foundation Medicine     |               | Google         |             |
| Health & wellness | Freenome                |               | Google         |             |
| Health & wellness | Vida Health             |               | Google         |             |
| Health & wellness | PatientPing             |               | Google         |             |
| Health & wellness | Aledade                 |               | Google         |             |
| Health & wellness | Hello Heart             |               | Google         |             |
| Health & wellness | Zephyr Health           |               | Google         |             |
| Health & wellness | Walker & Company Brands |               | Google         |             |
| Health & wellness | ZappRx                  |               | Google         |             |
| Health & wellness | Spruce Health           |               | Google         |             |
| Health & wellness | Aspire Health           |               | Google         |             |
| Health & wellness | Orange Chef             |               | Google         |             |
| Health & wellness | Predilytics             |               | Google         |             |
| Health & wellness | Oration                 |               | Google         |             |
| Health & wellness | TinyRx                  |               | Google         |             |
| Health & wellness | FitStar                 |               | Google         | Fitbit      |
| Health & wellness | Navigenics              |               | Google         |             |
| Health & wellness | 1Life Healthcare        |               | Google         |             |

| CATEGORY          | NAME                       | SUBSIDIARY OF | INVESTED IN BY | ACQUIRED BY |
|-------------------|----------------------------|---------------|----------------|-------------|
| Health & wellness | FogPharma                  |               | Google         |             |
| Health & wellness | Wingu                      |               | Google         |             |
| Health & wellness | Qliance Medical Management |               |                | Amazon      |
| Health & wellness | Zocdoc                     |               |                | Amazon      |
| Health & wellness | Doctor on Demand           |               | Google         |             |
| Health & wellness | Senosis Health             |               |                | Google      |
| Health & wellness | Lift Labs                  |               |                | Google      |
| Health & wellness | Fractyl Laboratories       |               | Google         |             |
| Health & wellness | Rare Light                 |               |                | Apple       |
| Health & wellness | Editas Medicine            |               | Google         |             |
| Health & wellness | DNAnexus                   |               | Google         |             |
| Health & wellness | Relay Therapeutics         |               | Google         |             |
| Health & wellness | Rani Therapeutics          |               | Google         |             |
| Health & wellness | Spero Therapeutics         |               | Google         |             |
| Health & wellness | Celsius Therapeutics       |               | Google         |             |
| Health & wellness | LifeMine Therapeutics      |               | Google         |             |
| Health & wellness | Rodin Therapeutics         |               | Google         |             |
| Health & wellness | Carrick Therapeutics       |               | Google         |             |
| Home goods        | Move Loot                  |               | Google         |             |
| Infrastructure    | Poynt                      |               | Google         |             |
| Infrastructure    | Puppet                     |               | Google         |             |
| Infrastructure    | Stackdriver                |               |                | Google      |
| Infrastructure    | Metaweb Technologies       |               |                | Google      |
| Infrastructure    | Union Bay Networks         |               |                | Apple       |
| Infrastructure    | Equinix                    |               | Microsoft      |             |
| Infrastructure    | SmartPipes                 |               | Microsoft      |             |
| Internet          | Google                     |               | Google         |             |
| Internet          | Alphabet                   |               | Google         |             |
| IOT               | Nest Labs                  |               | Google         |             |
| IOT               | Sidewalk Labs              | Google        |                |             |
| IOT               | Nest                       | Google        |                |             |
| IOT               | 2lemetry                   |               |                | Amazon      |
| IOT               | Styleware                  |               |                | Apple       |
| IOT               | Nest Labs                  |               |                | Google      |
| Manufacturing     | Carbon                     |               | Google         |             |

| CATEGORY          | NAME                       | SUBSIDIARY OF | INVESTED IN BY | ACQUIRED BY |
|-------------------|----------------------------|---------------|----------------|-------------|
| Manufacturing     | Veo Robotics               |               | Google         |             |
| Manufacturing     | Plethora                   |               | Google         |             |
| Manufacturing     | CircuitHub                 |               | Google         |             |
| Manufacturing     | HTC-Pixel Phone Division   |               |                | Google      |
| Manufacturing     | Channel Intelligence       |               |                | Google      |
| Manufacturing     | InVisage Technologies      |               |                | Apple       |
| Manufacturing     | Passif Semiconductor       |               |                | Apple       |
| Manufacturing     | PF Semi                    |               |                | Apple       |
| Manufacturing     | Intrinsity                 |               |                | Apple       |
| Manufacturing     | Beats Electronics          |               |                | Apple       |
| Manufacturing     | Corning Incorporated       |               | Apple          |             |
| Manufacturing     | Perbix                     |               |                | Tesla       |
| Manufacturing     | Riviera Tool LLC           |               |                | Tesla       |
| Manufacturing     | Grohmann Engineering       |               |                | Tesla       |
| Manufacturing     | Alta Motors                |               | Tesla          |             |
| Manufacturing     | Pacific Microsonics        |               |                | Microsoft   |
| Real estate       | HomeLight                  |               | Google         |             |
| Real estate       | Cozy                       |               | Google         |             |
| Real estate       | Airbnb                     |               |                | Amazon      |
| Security          | eMagin                     |               | Apple          |             |
| Security          | LegbaCore                  |               |                | Apple       |
| Space exploration | SpaceX                     |               |                | Elon Musk   |
| Space exploration | Planetary Resources        |               | Eric Schmidt   |             |
| Space exploration | Planetary Resources        |               | Larry Page     |             |
| Telecomms         | Imagination Technologies   |               | Apple          |             |
| Telecomms         | Imagination Technologies   |               | Apple          |             |
| Telecomms         | Internet.org (Free Basics) | Facebook      |                |             |
| Telecomms         | Endaga                     |               |                | Facebook    |
| Telecomms         | Orbital Insight, Inc.      |               | Google         |             |
| Telecomms         | O3b Networks               |               | Google         |             |
| Telecomms         | Orion Network Systems      |               |                | Apple       |
| Telecomms         | Google Fiber               | Google        |                |             |
| Telecomms         | Dialpad                    |               | Google         |             |
| Telecomms         | Helium                     |               | Google         |             |
| Telecomms         | Clearwire                  |               | Google         |             |
| Telecomms         | Ubiquisys                  |               | Google         |             |

| CATEGORY       | NAME                    | SUBSIDIARY OF | INVESTED IN BY | ACQUIRED BY |
|----------------|-------------------------|---------------|----------------|-------------|
| Telecomms      | GrandCentral            |               |                | Google      |
| Telecomms      | modu                    |               |                | Google      |
| Telecomms      | SayNow                  |               |                | Google      |
| Telecomms      | Motorola Mobility       |               |                | Google      |
| Telecomms      | Limes Audio             |               |                | Google      |
| Telecomms      | Finisar                 |               | Apple          |             |
| Telecomms      | 2nd Century             |               | Microsoft      |             |
| Telecomms      | Nokia                   |               |                | Microsoft   |
| Telecomms      | Navic Systems           |               |                | Microsoft   |
| Telecomms      | Skype                   |               |                | Microsoft   |
| Transportation | Urban Engines           |               |                | Google      |
| Transportation | Waze                    |               |                | Google      |
| Transportation | Tesla                   |               | Google         |             |
| Transportation | Aptera                  |               | Google         |             |
| Transportation | Openbay                 |               | Google         |             |
| Transportation | ZipDash                 |               |                | Google      |
| Transportation | Tesla                   |               |                |             |
| Transportation | Playment                |               | Google         |             |
| Transportation | Scotty Labs             |               | Google         |             |
| Transportation | Uber                    |               |                | Amazon      |
| Transportation | Kitty Hawk              |               | Larry Page     |             |
| Transportation | Uber                    |               | Microsoft      |             |
| Transportation | Embark                  |               |                | Apple       |
| Transportation | HopStop                 |               |                | Apple       |
| Transportation | Didi Chuxing            |               | Apple          |             |
| Transportation | The Boring Company      | Tesla         |                |             |
| Wearables      | Magic Leap              |               | Google         |             |
| Wearables      | Bloom                   |               | Google         |             |
| Wearables      | WIMM Labs               |               |                | Google      |
| Wearables      | Cronologics Corporation |               |                | Google      |
| Wearables      | Eyefluence              |               |                | Google      |
| Wearables      | Vocal IQ                |               |                | Apple       |



# NOTES

## INTRODUCTION

1. Peter Cohen, "Macworld Expo Attendance Breaks Records," *Macworld*, March 13, 2007, retrieved June 27, 2018, <https://www.macworld.com/article/1056750/macworldexpo.html>.
2. "Steve Jobs iPhone 2007 Presentation," YouTube, May 13, 2013, retrieved June 23, 2018, <https://www.youtube.com/watch?v=vN4U5FqrOdQ>.
3. Judy Bachrach, "WikiHistory: Did the Leaks Inspire the Arab Spring?" *World Affairs Journal*, July/August 2011, retrieved August 5, 2018, <http://www.worldaffairsjournal.org/article/wikihistory-did-leaks-inspire-arab-spring>.
4. Issie Lapowsky, "Facebook Exposed 87 Million Users to Cambridge Analytica," *WIRED*, April 4, 2018, retrieved December 16, 2018, <https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/>.
5. "iPhone Sales Said to Hit Half-Million," CNN Money, July 2, 2007, retrieved June 23, 2018, [http://money.cnn.com/2007/07/02/technology/iphone\\_sales/](http://money.cnn.com/2007/07/02/technology/iphone_sales/).
6. Dawn Chmielewski, "The Wait Is Over: The Scene from 2007 When the iPhone First Went on Sale," *Los Angeles Times*, June 30, 2007, retrieved June 23, 2018, <http://www.latimes.com/business/technology/la-fi-iphone-debut-20070630-story.html>.
7. "Number of Smartphone Users Worldwide from 2014 to 2020 (in Billions)," Statista, n.d., retrieved June 27, 2018, <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>.
8. "Transcript of Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention," Microsoft News, February 14, 2017, retrieved January 30, 2019, <https://news.microsoft.com/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf>.
9. Alexis Wichowski, "Net States Rule the World: Ignore Them at Your Peril," *WIRED*, November 4, 2017, retrieved April 7, 2019, <https://www.wired.com/story/net-states-rule-the-world-we-need-to-recognize-their-power/>.
10. Gary Davis, "Silk Road's 'Libertas'? 5 Fast Facts You Need to Know," Heavy (website), December 2013, retrieved November 25, 2018, <https://heavy.com/news/2013/12/gary-davis-silk-road-2-arrests-libertas/>.
11. Aaron Rogan, "Irishman Gary Davis Denies Helping to Run Silk Road Dark Net Website," *Times* (UK), August 24, 2018, retrieved November 25, 2018, <https://www>.

- thetimes.co.uk/article/irishman-gary-davis-denies-helping-to-run-silk-road-dark-net-website-3fk93r7bl.
12. Aaron Rogan, "Irishman Gary Davis Denies Helping to Run Silk Road Dark Net Website," *Times (UK)*, August 24, 2018, retrieved February 5, 2019, <https://www.thetimes.co.uk/article/irishman-gary-davis-denies-helping-to-run-silk-road-dark-net-website-3fk93r7bl>.
  13. Steve Kovach, "FBI Says Illegal Drugs Marketplace Silk Road Generated \$1.2 Billion in Sales Revenue," *Business Insider*, October 2, 2013, retrieved February 2, 2019, <https://www.businessinsider.com/silk-road-revenue-2013-10>.
  14. John Biggs, "Alleged Top Moderators of Silk Road 2 Forums Arrested in Ireland, U.S. in International Sweep," *TechCrunch*, December 20, 2013, retrieved February 5, 2019, <https://techcrunch.com/2013/12/20/alleged-top-moderator-of-silk-road-2-forums-arrested-in-ireland/>.
  15. 47 U.S. Code § 230, "Protection for Private Blocking and Screening of Offensive Material," Communications Decency Act, 1996, Legal Information Institute, retrieved February 2, 2019, <https://www.law.cornell.edu/uscode/text/47/230>.
  16. *United States of America v. Microsoft Corporation*, 253 F.3d 34 (DC Cir. 2001), Justia Legal Resources, US Federal Law, retrieved February 5, 2019, <https://law.justia.com/cases/federal/appellate-courts/F3/253/34/576095>.
  17. Kate Conger, "Google Plans Not to Renew Its Contract for Project Maven, a Controversial Pentagon Drone AI Imaging Program," *Gizmodo Media Group*, June 1, 2018, retrieved December 2, 2018, <https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620?rev=1527878336532>.
  18. Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," US Department of Defense, July 21, 2017, retrieved December 2, 2018, <https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/>.
  19. Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," US Department of Defense, July 21, 2017, retrieved July 3, 2019, <https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/>.
  20. Kate Conger, "Google Plans Not to Renew Its Contract for Project Maven, a Controversial Pentagon Drone AI Imaging Program," *Gizmodo Media Group*, June 1, 2018, retrieved December 2, 2018, <https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620?rev=1527878336532>.
  21. Kate Conger, "Google Employees Resign in Protest Against Pentagon Contract," *Gizmodo Media Group*, May 14, 2018, retrieved December 2, 2018, <https://gizmodo.com/google-employees-resign-in-protest-against-pentagon-con-1825729300>.
  22. Daisuke Wakabayashi, "Google Will Not Renew Pentagon Contract That Upset Employees," *New York Times*, June 1, 2018, retrieved December 2, 2018, <https://static01.nytimes.com/files/2018/technology/googleletter.pdf>.
  23. "Anonymous Claims to Have Taken Down 20,000 IS Twitter Accounts," *BBC News*, November 20, 2015, retrieved May 11, 2018, <http://www.bbc.co.uk/newsbeat/article/34877968/anonymous-claims-to-have-taken-down-20000-is-twitter-accounts>.
  24. J. M. Berger, "The Evolution of Terrorist Propaganda: The Paris Attack and Social Media," *Brookings Institution*, January 27, 2015, retrieved May 11, 2018, <https://www.brookings.edu/testimonies/the-evolution-of-terrorist-propaganda-the-paris-attack-and-social-media/>.
  25. Micah Sifry, "Ambient Awareness," *Civichall*, June 18, 2019, retrieved June 23, 2019, <https://civichall.org/civichall/ambient-awareness/>.
  26. "Facial Recognition System Helps Trace 3,000 Missing Children in 4 Days," *NDTV*, April 22, 2018, retrieved May 30, 2018, <https://www.ndtv.com/india-news/facial-recognition-system-helps-trace-3-000-missing-children-in-4-days-1841192?pffrom=home>.

topstories.

27. Gabrielle Fonrouge, "Teens Caught in Rough Surf Saved in First Drone Rescue of Its Kind," *New York Post*, January 18, 2018, retrieved May 30, 2018, <https://nypost.com/2018/01/18/drone-makes-first-ever-water-rescue-for-teens-caught-in-rough-surf/>.
28. Mitchell Broussard, "Tim Cook Shares Lifesaving Apple Watch Story After Teen Goes into Kidney Failure," *MacRumors*, May 1, 2018, retrieved May 30, 2018, <https://www.macrumors.com/2018/05/01/tim-cook-apple-watch-kidney-failure/>.
29. Henry David Thoreau, *Civil Disobedience* (Nashville: American Renaissance Books, 2010), 23.

## CHAPTER 1: RISE OF THE CITIZEN-USER

1. Thomas Juster, "Changing Times of American Youth: 1981–2003," Institute for Social Research, University of Michigan, November 2004, retrieved September 9, 2018, [http://ns.umich.edu/Releases/2004/Nov04/teen\\_time\\_report.pdf](http://ns.umich.edu/Releases/2004/Nov04/teen_time_report.pdf).
2. "Prices in the Eighties," In the 80s (website), n.d., retrieved September 9, 2018, <http://www.inthe80s.com/prices.shtml>.
3. Stewart Wolpin, "The First Cellphone Went on Sale 30 Years Ago for \$4,000," *Mashable*, March 13, 2014, retrieved <https://mashable.com/2014/03/13/first-cellphone-on-sale/>; CPI Inflation Calculator, "U.S. Inflation Rate, \$4,000 in 1985 to 2019," retrieved June 23, 2019, <http://www.in2013dollars.com/us/inflation/1985?amount=4000>
4. Scott Brown, "WarGames: A Look Back at the Film That Turned Geeks and Phreaks into Stars," *WIRED*, July 21, 2008, retrieved September 9, 2018, <https://www.wired.com/2008/07/ff-wargames/>.
5. "Sir Tim Berners-Lee," National Portrait Gallery, n.d., retrieved April 14, 2019, <https://www.npg.org.uk/collections/search/person/mp58761/sir-tim-berners-lee>.
6. "Number of Smartphone Users Worldwide from 2014 to 2020 (in Billions)," Statista, n.d., retrieved September 12, 2018, <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>.
7. Steven Levy, *Hackers: Heroes of the Computer Revolution* (Garden City, NY: Anchor Press/Doubleday, 1984), 26–36.
8. "Why Half of Developers Don't Have a Computer Science Degree," Next Web, April 23, 2016, retrieved November 25, 2018, <https://thenextweb.com/insider/2016/04/23/dont-need-go-college-anymore-programmer/>.
9. Christopher Lehmann-Haupt, "Books of the Times; Hackers as Heroes," *New York Times*, December 24, 1984, retrieved September 9, 2018, <https://www.nytimes.com/1984/12/24/books/books-of-the-times-hackers-as-heroes.html>.
10. Faubrice Florin, *Hackers: Wizards of the Electronic Age* (documentary), 1985, retrieved September 9, 2018, <https://www.youtube.com/watch?v=zOP1LNr70aU>.
11. Carole Cadwalladr, "Stewart Brand's 'Whole Earth Catalog,' the Book That Changed the World," *Guardian*, May 4, 2013, retrieved May 20, 2018, <https://www.theguardian.com/books/2013/may/05/stewart-brand-whole-earth-catalog>.
12. "Stewart Brand States Information Wants to Be Free," Getty Images, November 1, 1984, retrieved September 9, 2018, <https://www.gettyimages.com/detail/video/at-the-first-hackers-conference-in-1984-steve-wozniak-and-news-footage/146496695>.
13. Joshua Gans, "'Information Wants to Be Free': The History of That Quote," *Digitopoly* (blog), 25 Oct. 2015, [www.digitopoly.org/2015/10/25/information-wants-to-be-free-the-history-of-that-quote/](http://www.digitopoly.org/2015/10/25/information-wants-to-be-free-the-history-of-that-quote/).
14. This is an idea I first explored in a book chapter on information-sharing and diplomacy: Alexis Wichowski, "'Secrecy Is for Losers': How Diplomats Should Embrace Openness to Protect National Security," in *Digital Diplomacy: Theory and Practice*, ed. Marcus Holmes and Corneliu Bjola (London and New York: Routledge, 2016).
15. "Mission Statement," *Economist*, June 2, 2009, retrieved November 25, 2018, <https://www.economist.com/news/2009/06/02/mission-statement>.

16. "From the Garage to the Googleplex," *Google: Our Story*, n.d., retrieved November 25, 2018, <https://www.google.com/about/our-story/>.
17. Christian Zibreg, "Mark Zuckerberg Says You Need to 'Move Fast and Break Things,'" *Geek*, October 2, 2009, retrieved November 25, 2018, <https://www.geek.com/news/mark-zuckerberg-says-you-need-to-move-fast-and-break-things-922432/>.
18. Anna Wiener, "The Complicated Legacy of Stewart Brand's 'Whole Earth Catalog,'" *New Yorker*, November 18, 2018, retrieved November 25, 2018, <https://www.newyorker.com/news/letter-from-silicon-valley/the-complicated-legacy-of-stewart-brands-whole-earth-catalog>.
19. "Home Computers and Internet Use in the United States: August 2000," US Census Bureau, September 2001, retrieved September 9, 2018, <https://www.census.gov/prod/2001pubs/p23-207.pdf>.
20. Bill Gates, "Content Is King," Microsoft, January 1996, retrieved via Wayback Machine on June 27, 2018, <http://web.archive.org/web/20010126005200/http://www.microsoft.com/billgates/columns/1996essay/essay960103.asp>.
21. Farhad Manjoo, "Jurassic Web," *Slate*, February 24, 2009, retrieved June 27, 2018, [http://www.slate.com/articles/technology/technology/2009/02/jurassic\\_web.html](http://www.slate.com/articles/technology/technology/2009/02/jurassic_web.html).
22. "Historical Daily Viewing Activity Among Households & Persons 2+," Nielsen Company, n.d., retrieved June 27, 2018, <http://www.nielsen.com/content/dam/corporate/us/en/newswire/uploads/2009/11/historicalviewing.pdf>.
23. "The Best Websites of 1996," *TIME*, June 24, 2001, retrieved June 27, 2018, <http://content.time.com/time/magazine/article/0,9171,135245,00.html>.
24. Tim O'Reilly, "What Is Web 2.0?" O'Reilly Media, September 30, 2005, retrieved July 1, 2018, <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>.
25. Gary Marshall, "Happy Birthday, Windows 95: The OS That Changed It All," *TechRadar*, August 24, 2015, retrieved July 1, 2018, <https://www.techradar.com/news/software/operating-systems/happy-birthday-windows-95-the-os-that-changed-it-all-711984>.
26. Lance Ulanoff, "Remembering the Windows 95 Launch: A Triumph of Marketing," *Mashable*, August 24, 2015, retrieved June 27, 2018, <https://mashable.com/2015/08/24/remembering-windows-95-launch/#X9YZEiwCSiqB>.
27. Ian Morris, "Seven Ways Windows 95 Changed the World," *Forbes*, August 24, 2015, retrieved June 27, 2018, <https://www.forbes.com/sites/ianmorris/2015/08/24/windows-95-changed-the-world/>.
28. Alyssa Newcomb, "Why Windows 95 Was a Game-Changer for Computer Users Everywhere," *ABC News*, August 24, 2015, retrieved July 1, 2018, <https://abcnews.go.com/Technology/windows-95-game-changer-computer-users/story?id=33212036>.
29. Brian Feldman, "U.S. v. *Microsoft* Proved That Antitrust Can Keep Tech Power in Check," *New York* magazine, December 12, 2017, retrieved July 1, 2018, <http://nymag.com/selectall/2017/12/u-s-v-microsoft-proved-that-antitrust-can-check-tech-power.html>.
30. Michael Calore, "April 22, 1993: Mosaic Browser Lights Up Web with Color, Creativity," *WIRED*, April 22, 2010, retrieved July 1, 2018, <https://www.wired.com/2010/04/0422mosaic-web-browser/>.
31. Sean Cooper, "Whatever Happened to Netscape?" *Engadget*, May 10, 2014, retrieved July 1, 2018, <https://www.engadget.com/2014/05/10/history-of-netscape/>.
32. "AOL, Netscape Tie Knot," *CNN Money*, November 24, 1998, retrieved July 1, 2018, <http://money.cnn.com/1998/11/24/technology/aol/>.
33. Luisa Kroll, "The World's Billionaires: 25th Anniversary Timeline," *Forbes*, March 7, 2012, retrieved July 1, 2018, <https://www.forbes.com/special-report/2012/billionaires-25th-anniversary-timeline.html>.
34. Brian Feldman, "U.S. v. *Microsoft* Proved That Antitrust Can Keep Tech Power in Check," *New York Magazine*, December 12, 2017, <http://nymag.com/intelligencer/2017/12/u-s-v-microsoft-proved-that-antitrust-can-check-tech-power.html>.
35. Désiré Athow, "Microsoft's Lawsuit Payouts Amount to Around \$9 Billion," *In-*

- quirer, July 14, 2005, retrieved July 1, 2018, <https://www.theinquirer.net/inquirer/news/1048246/microsoft-lawsuit-payouts-usd9-billion>.
36. "AT&T Breakup II: Highlights in the History of a Telecommunications Giant," *Los Angeles Times*, September 21, 1995, retrieved July 1, 2018, [http://articles.latimes.com/1995-09-21/business/fi-48462\\_1\\_system-breakup](http://articles.latimes.com/1995-09-21/business/fi-48462_1_system-breakup).
  37. "May 15, 1911: Supreme Court Orders Standard Oil to Be Broken Up," *New York Times*, May 25, 2012, retrieved July 1, 2018, <https://learning.blogs.nytimes.com/2012/05/15/may-15-1911-supreme-court-orders-standard-oil-to-be-broken-up/>.
  38. Joseph Nocera, "His Own Worst Enemy," *Fortune*, December 7, 1998, retrieved June 23, 2019, [http://archive.fortune.com/magazines/fortune/fortune\\_archive/1998/12/07/252139/index.htm](http://archive.fortune.com/magazines/fortune/fortune_archive/1998/12/07/252139/index.htm).
  39. Brian Feldman, "U.S. v. Microsoft Proved That Antitrust Can Keep Tech Power in Check," *New York magazine*, December 12, 2017, retrieved July 1, 2018, <http://nymag.com/selectall/2017/12/u-s-v-microsoft-proved-that-antitrust-can-check-tech-power.html>.
  40. "Final Judgment Civil Action No. 98-1232 (CKK)," US Department of Justice, n.d., retrieved July 1, 2018, <https://www.justice.gov/atr/case-document/final-judgment-133>; Anna Domanska, "The Famous History of Microsoft's Antitrust Case," *Industry Leaders*, February 12, 2018, retrieved July 1, 2018, <https://www.industryleadersmagazine.com/famous-history-microsofts-antitrust-case/>; Nancy Gohring, "End of an Era: Microsoft Antitrust Oversight Ends," *Macworld*, May 11, 2011, retrieved July 1, 2018, [https://www.macworld.com/article/1159841/microsoft\\_antitrust.html](https://www.macworld.com/article/1159841/microsoft_antitrust.html).
  41. David Moschella, "Microsoft Losing in the Court of Public Opinion," *Computerworld*, May 22, 2000, retrieved July 1, 2018, <https://www.computerworld.com/article/2594627/app-development/microsoft-losing-in-the-court-of-public-opinion.html>.
  42. "Pirate Bay Founding Group Disbands," BBC News, June 28, 2010, retrieved May 20, 2018, <http://www.bbc.com/news/10433195>.
  43. "What Is the Pirate Agency?," Piratbyrå, February 9, 2004, retrieved May 22, 2018, <https://web.archive.org/web/20040209024510/http://piratbyran.org:80/index.php?view=articles&cat=8>.
  44. Patrick Burkart, *Pirate Politics: The New Information Policy Contests* (Cambridge, MA: MIT Press, 2014), 17.
  45. Tom Lamont, "Napster: The Day the Music Was Set Free," *Guardian*, February 23, 2013, retrieved May 20, 2018, <https://www.theguardian.com/music/2013/feb/24/napster-music-free-file-sharing>.
  46. Paul Resnikoff, "Pressure Intensifies as the Pirate Bay Crosses 300 Million Visitors," *Digital Music News*, June 11, 2017, retrieved May 20, 2018, <https://www.digitalmusic-news.com/2017/06/11/pressure-pirate-bay-300-million/>; home page, Pirate Bay, n.d., retrieved May 20, 2018, <https://thepiratebay.org/>.
  47. Jan Libbenga, "Pirate Bay Resurfaces, While Protesters Walk the Street," *Register*, June 5, 2006, retrieved September 12, 2018, [https://www.theregister.co.uk/Print/2006/06/05/pirate\\_bay\\_reemerges/](https://www.theregister.co.uk/Print/2006/06/05/pirate_bay_reemerges/).
  48. Ryan Neal, "The Pirate Bay Moves Again: How Many Domains Are Left?" *International Business Times*, December 18, 2013, retrieved May 20, 2018, <http://www.ibtimes.com/pirate-bay-moves-again-how-many-domains-are-left-1514306>; Christopher de Looper, "History of the Pirate Bay: Internet Outlaw or Internet File-Sharing Freedom Fighter?," *Tech Times*, December 17, 2014, retrieved May 20, 2018, <http://www.techtimes.com/articles/22362/20141217/history-pirate-bay.htm>.
  49. Julianne Pepitone, "The Pirate Bay Down in Extended Outage," *CNN Money*, October 3, 2012, retrieved May 20, 2018, <http://money.cnn.com/2012/10/02/technology/pirate-bay-down/index.html>.
  50. "About PPI," Pirate Parties International, n.d., retrieved May 20, 2018, <https://pp-international.net/about-ppi/>.
  51. "Julia Reda, Euro-Pirate: For DE, EU, WWW, and Human Rights," Piraten Partei

- Deutschland, n.d., retrieved May 20, 2018, <https://www.piratenpartei.de/partei/julia-reda/>; "European Parliament 2019 Elections Results," Bloomberg, June 23, 2019, retrieved June 23, 2019, <https://www.bloomberg.com/graphics/2019-european-parliament-elections/>.
52. "Iceland: Individual-Taxes on Personal Income," Pricewaterhouse Coopers, n.d., retrieved July 20, 2018, <http://taxsummaries.pwc.com/ID/Iceland-Individual-Taxes-on-personal-income>; Jon Henley, "Iceland PM Steps Aside After Protests over Panama Papers Revelations," *Guardian*, April 5, 2016, retrieved June 3, 2018, <https://www.theguardian.com/world/2016/apr/05/iceland-prime-minister-resigns-over-panama-papers-revelations>.
  53. "Iceland's Pirate Party Invited to Form Government," *Guardian*, December 2, 2016, retrieved May 20, 2018, <https://www.theguardian.com/world/2016/dec/02/iceland-pirate-party-invited-form-government-coalition>.
  54. Derek Thompson, "Google's CEO: 'The Laws Are Written by Lobbyists'" *Atlantic*, October 1, 2010, retrieved November 23, 2018, <https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/>.
  55. "Facebook: Facts & Figures for 2010," *Digital Buzz* (blog), March 22, 2010, retrieved November 25, 2018, <http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/>.
  56. Rebecca Rosen, "So, Was Facebook Responsible for the Arab Spring After All?," *Atlantic*, September 23, 2011, retrieved November 25, 2018, <https://www.theatlantic.com/technology/archive/2011/09/so-was-facebook-responsible-for-the-arab-spring-after-all/244314/>.
  57. Aaron Smith, "Smartphone Adoption and Usage," Pew Research Center: Internet and Technology, July 11, 2011, retrieved November 25, 2018, <http://www.pewinternet.org/2011/07/11/smartphone-adoption-and-usage/>.
  58. K. S. Young, "Internet Addiction: A New Clinical Phenomenon and Its Consequences," *American Behavioral Scientist* 48, no. 4 (2004): 402–15.
  59. C. Shirky, "The Political Power of Social Media: Technology, the Public Sphere, and Political Change," *Foreign Affairs* (2011): 28–41.
  60. Technically, it's Habermas's "habilitation thesis," the European equivalent of a doctoral dissertation; it's the final requirement one must pass in order to be able to teach as a professor in a European university.
  61. Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Cambridge, MA: MIT Press, 1962/1989).
  62. Thomas File, "Voting in America: A Look at the 2016 Presidential Election," US Census Bureau, May 10, 2017, retrieved May 20, 2018, [https://www.census.gov/newsroom/blogs/random-samplings/2017/05/voting\\_in\\_america.html](https://www.census.gov/newsroom/blogs/random-samplings/2017/05/voting_in_america.html).
  63. Gregory Wallace, "Voter Turnout at 20-Year Low in 2016," CNN, November 30, 2016, retrieved May 20, 2018, <https://www.cnn.com/2016/11/11/politics/popular-vote-turnout-2016/index.html>.
  64. Charlotte Alter, "Voter Turnout in Midterm Elections Hits 72-Year Low," *TIME*, November 10, 2014, retrieved May 20, 2018, <http://time.com/3576090/midterm-elections-turnout-world-war-two/>.
  65. Philip Bump, "Donald Trump Will Be President Thanks to 80,000 People in Three States," *Washington Post*, December 1, 2016, retrieved May 20, 2018, [https://www.washingtonpost.com/news/the-fix/wp/2016/12/01/donald-trump-will-be-president-thanks-to-80000-people-in-three-states/?noredirect=on&utm\\_term=.8d271fef3166](https://www.washingtonpost.com/news/the-fix/wp/2016/12/01/donald-trump-will-be-president-thanks-to-80000-people-in-three-states/?noredirect=on&utm_term=.8d271fef3166); "Average Annual Population of NYC Neighborhoods, 2011–2015," New York State Department of Health, n.d., retrieved May 20, 2018, <https://www.health.ny.gov/statistics/cancer/registry/appendix/neighborhoodpop.htm>.
  66. "Mobile Fact Sheet," Pew Research Center: Internet and Technology, June 12, 2019, retrieved July 3, 2019, <http://www.pewinternet.org/fact-sheet/mobile/>.
  67. Tina Lu, "Smartphone Users Replace Their Device Every Twenty-One Months," Coun-

- terpoint Research, October 13, 2017, retrieved June 3, 2018, <https://www.counterpointresearch.com/smartphone-users-replace-their-device-every-twenty-one-months/>.
68. Linda Poon, "Why Won't You Be My Neighbor?," CityLab, August 19, 2015, retrieved June 3, 2018, <https://www.citylab.com/equity/2015/08/why-wont-you-be-my-neighbor/401762/>.
  69. Aaron Smith, "U.S. Smartphone Use in 2015," Pew Research Center: Internet and Technology, April 1, 2015, retrieved on May 20, 2018, <http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/>.
  70. Katherine Stewart, "Online Voting: The Solution to Declining Political Engagement?," RAND, March 2018, retrieved May 20, 2018, <https://www.rand.org/blog/2018/03/online-voting-the-solution-to-declining-political-engagement.html>.
  71. "Voting and Registration in the Election of November 2008," US Census Bureau, July 2012, retrieved May 20, 2018, <https://www.census.gov/prod/2010pubs/p20-562.pdf>.
  72. Paul Hiebert, "Half of Young People Hold onto Their Phone Throughout the Day," YouGov, July 6, 2016, retrieved May 20, 2018, <https://today.yougov.com/topics/lifestyle/articles-reports/2016/07/06/young-people-carry-phone-in-hand>.
  73. Shannon Liao, "Google Admits It Tracked User Location Data Even When the Setting Was Turned Off," Verge, November 21, 2017, retrieved May 20, 2018, <https://www.theverge.com/2017/11/21/16684818/google-location-tracking-cell-tower-data-android-os-firebase-privacy>.
  74. Gopal Sathe, "It's Not Just Facebook, All Apps Are Scooping Up Your Data," Gadgets NDTV, March 28, 2018, retrieved June 3, 2018, <https://gadgets.ndtv.com/apps/features/its-not-just-facebook-all-apps-are-scooping-up-your-data-1829861>.
  75. Narseo Vallina-Rodriguez, "7 in 10 Smartphone Apps Share Your Data with Third-Party Services," *Scientific American*, May 30, 2017, retrieved June 3, 2018, <https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/>.
  76. Rick Noack, "How Long Would It Take to Read the Terms of Your Smartphone Apps? These Norwegians Tried It Out," *Washington Post*, May 28, 2016, retrieved June 3, 2018, [https://www.washingtonpost.com/news/worldviews/wp/2016/05/28/how-long-would-it-take-to-read-the-terms-of-your-smartphone-apps-these-norwegians-tried-it-out/?utm\\_term=.e440a179ba77](https://www.washingtonpost.com/news/worldviews/wp/2016/05/28/how-long-would-it-take-to-read-the-terms-of-your-smartphone-apps-these-norwegians-tried-it-out/?utm_term=.e440a179ba77).
  77. Andy Greenberg, "Who Reads the Fine Print Online? Less Than One Person in 1000," *Forbes*, April 8, 2010, retrieved June 2, 2018, <https://www.forbes.com/sites/firewall/2010/04/08/who-reads-the-fine-print-online-less-than-one-person-in-1000/#1c2a32967017>.
  78. Buckminster Fuller, "2025, If . . ." *Whole Earth Catalog*, Spring 1975, retrieved June 2, 2018, <http://www.wholeearth.com/issue/2005/article/94/2025.if>.

## CHAPTER 2: NET STATES IRL

1. Robinson Meyer, "What's Happening with the Relief Effort in Puerto Rico?" *Atlantic*, October 4, 2017, retrieved November 15, 2017, [www.theatlantic.com/science/archive/2017/10/what-happened-in-puerto-rico-a-timeline-of-hurricane-maria/541956/](http://www.theatlantic.com/science/archive/2017/10/what-happened-in-puerto-rico-a-timeline-of-hurricane-maria/541956/).
2. Mindy Weisberger, "Harvey vs. Katrina: How Do These Monster Storms Compare?" *LiveScience*, August 29, 2017, retrieved November 15, 2017, [www.livescience.com/60257-harvey-vs-katrina-storm-comparison.html](http://www.livescience.com/60257-harvey-vs-katrina-storm-comparison.html).
3. Brian Resnick, "Why Hurricane Maria Is Such a Nightmare for Puerto Rico," *Vox*, September 21, 2017, retrieved November 15, 2017, [www.vox.com/science-and-health/2017/9/21/16345176/hurricane-maria-2017-puerto-rico-san-juan-meteorology-wind-rain-power](http://www.vox.com/science-and-health/2017/9/21/16345176/hurricane-maria-2017-puerto-rico-san-juan-meteorology-wind-rain-power).
4. "Historic Hurricane Harvey's Recap," Weather Channel, August 29, 2017, retrieved November 15, 2017, [weather.com/storms/hurricane/news/tropical-storm-harvey-forecast-texas-louisiana-arkansas](http://weather.com/storms/hurricane/news/tropical-storm-harvey-forecast-texas-louisiana-arkansas).

5. Eva Moravec, "Texas Officials: Hurricane Harvey Death Toll at 82, 'Mass Casualties Have Absolutely Not Happened,'" *Washington Post*, September 14, 2017, retrieved August 5, 2018, [https://www.washingtonpost.com/national/texas-officials-hurricane-harvey-death-toll-at-82-mass-casualties-have-absolutely-not-happened/2017/09/14/bff3ffea-9975-11e7-87fc-c3f7ee4035c9\\_story.html?utm\\_term=.168ee7353810](https://www.washingtonpost.com/national/texas-officials-hurricane-harvey-death-toll-at-82-mass-casualties-have-absolutely-not-happened/2017/09/14/bff3ffea-9975-11e7-87fc-c3f7ee4035c9_story.html?utm_term=.168ee7353810).
6. "Historic Disaster Response to Hurricane Harvey in Texas," Federal Emergency Management Agency, September 22, 2017, retrieved May 30, 2018, <https://www.fema.gov/news-release/2017/09/22/historic-disaster-response-hurricane-harvey-texas>.
7. Nishant Kishore et al., "Mortality in Puerto Rico After Hurricane Maria," *New England Journal of Medicine*, May 29, 2018, retrieved May 30, 2018, <https://www.nejm.org/doi/full/10.1056/NEJMsa1803972>.
8. Luis Ferré-Sadurní, "In Puerto Rico, the Storm 'Destroyed Us,'" *New York Times*, September 21, 2017, retrieved May 11, 2018, <https://www.nytimes.com/2017/09/21/us/hurricane-maria-puerto-rico.html>.
9. Nishant Kishore et al., "Mortality in Puerto Rico After Hurricane Maria," *New England Journal of Medicine*, May 29, 2018, retrieved August 5, 2018, <https://www.nejm.org/doi/full/10.1056/NEJMsa1803972>.
10. "DoD Accelerates Hurricane Relief, Response Efforts in Puerto Rico," US Department of Defense, September 30, 2017, retrieved November 15, 2017, [www.defense.gov/News/Article/Article/1330501/dod-accelerates-hurricane-relief-response-efforts-in-puerto-rico](http://www.defense.gov/News/Article/Article/1330501/dod-accelerates-hurricane-relief-response-efforts-in-puerto-rico).
11. Julia Jacabo, "Hurricane Maria Death Toll Jumps to 34 in Puerto Rico," ABC News, October 3, 2017, retrieved December 11, 2018, <https://abcnews.go.com/US/hurricane-maria-death-toll-jumps-34-puerto-rico/story?id=50267118>; Alexis Campbell, "FEMA Has Yet to Authorize Full Disaster Help for Puerto Rico," Vox, October 16, 2017, retrieved December 11, 2018, <https://www.vox.com/policy-and-politics/2017/10/3/16400510/fema-puerto-rico-hurricane>; Leanna Garfield, "Hurricane Maria Decimated Puerto Rico's Food Supply: Here's What the Island's Farms Look Like Now," Business Insider, September 29, 2017, retrieved December 11, 2018, <https://www.businessinsider.com/photos-hurricane-maria-puerto-rico-farms-damage-caribbean-2017-9>.
12. Brian Kahn, "Puerto Rico Has a Once in a Lifetime Opportunity to Rethink How It Gets Electricity," Earther (website), October 4, 2017, retrieved December 11, 2018, <https://earther.gizmodo.com/puerto-rico-has-a-once-in-a-lifetime-opportunity-to-ret-1819143446>.
13. Christina Mercer, "History of PayPal: 1998 to Now," Techworld, November 25, 2015, retrieved November 15, 2017, [www.techworld.com/picture-gallery/business/history-of-paypal-1998-now-3630386/](http://www.techworld.com/picture-gallery/business/history-of-paypal-1998-now-3630386/).
14. Ian Kar, "The Design That Got MIT Engineers the Top Spot at Elon Musk's Hyperloop Competition," Quartz, February 8, 2016, retrieved November 15, 2017, [www.qz.com/611000/the-design-that-got-mit-engineers-the-top-spot-at-elon-musks-hyperloop-competition/](http://www.qz.com/611000/the-design-that-got-mit-engineers-the-top-spot-at-elon-musks-hyperloop-competition/).
15. "SpaceX Dragon Docked to Space Station," NASA, May 5, 2015, retrieved November 15, 2017, [www.nasa.gov/mission\\_pages/station/multimedia/gallery/iss034e060718.html](http://www.nasa.gov/mission_pages/station/multimedia/gallery/iss034e060718.html).
16. Brian Fung, "Here's How Far Every Tesla Model S Can Go on a Single Charge," *Washington Post*, December 30, 2014, retrieved November 15, 2017, [www.washingtonpost.com/news/the-switch/wp/2014/12/30/heres-how-far-every-tesla-model-s-can-go-on-a-single-charge/?utm\\_term=.5574ef4d7c7c](http://www.washingtonpost.com/news/the-switch/wp/2014/12/30/heres-how-far-every-tesla-model-s-can-go-on-a-single-charge/?utm_term=.5574ef4d7c7c).
17. Elon Musk, "Making Life Multi-Planetary," *New Space* 6, no. 1 (March 1, 2018), retrieved May 11, 2018, <https://doi.org/10.1089/space.2018.29013.emu>.
18. "Cost and Payment Options," Tesla Support, n.d., retrieved December 11, 2018, [https://www.tesla.com/support/energy/learn/solar-panels/cost-and-payment-options](http://www.tesla.com/support/energy/learn/solar-panels/cost-and-payment-options).
19. Carmine Gallo, "Tesla's Elon Musk Lights Up Social Media with a TED Style Keynote," *Forbes*, May 4, 2015, retrieved May 11, 2018, <https://www.forbes.com/sites/carmin-egallo/2015/05/04/teslas-elon-musk-lights-up-social-media-with-a-ted-style-keynote/>.

20. Tony Moore, "Queensland's Solar Energy Uptake Dims," *Brisbane Times*, August 12, 2015, retrieved December 11, 2018, <https://www.brisbanetimes.com.au/national/queensland/queenslands-solar-uptake-dims-20150812-gixuy1.html>; Alison Brown, "Queensland City Tops National Solar Panel List," *Sydney Morning Herald*, June 16, 2018, retrieved December 11, 2018, <https://www.smh.com.au/environment/sustainability/queensland-city-tops-national-solar-panel-list-20180615-p4zlni.html>; Joshua Robertson, "Queensland Installs Australia's First Powerwall Battery for Solar Trial," *Guardian*, January 18, 2016, retrieved December 11, 2018, [www.theguardian.com/environment/2016/jan/18/queensland-installs-australias-first-powerwall-battery-for-solar-trial](http://www.theguardian.com/environment/2016/jan/18/queensland-installs-australias-first-powerwall-battery-for-solar-trial).
21. Peter Dockrill, "This Island in American Samoa Is Almost 100% Powered by Tesla Solar Panels," *Science Alert*, November 23, 2016, retrieved December 11, 2018, <https://www.sciencealert.com/this-island-in-american-samoa-is-almost-100-powered-by-tesla-solar-panels>.
22. Austin Carr, "The Real Story Behind Elon Musk's \$2.6 Billion Acquisition of SolarCity and What It Means for Tesla's Future—Not to Mention the Planet's," *Fast Company*, June 7, 2017, retrieved December 11, 2018, <https://www.fastcompany.com/40422076/the-real-story-behind-elon-musks-2-6-billion-acquisition-of-solarcity-and-what-it-means-for-teslas-future-not-to-mention-the-planets>.
23. Danielle Muoio, "Tesla Is Ramping Up Battery Production to Aid Puerto Rico—But Installations Costs Are Reportedly Skyrocketing," *Business Insider*, October 9, 2017, retrieved December 11, 2018, <https://www.insider.com/tesla-ramps-battery-production-puerto-rico-2017-10>.
24. "How Much Electricity on Average Do Homes in Your State Use? (Ranked by State)," *Electric Choice* (blog), n.d., retrieved December 11, 2018, <https://www.electricchoice.com/blog/electricity-on-average-do-homes/>.
25. Fred Lambert, "Tesla Powerwalls and Powerpacks Keep the Lights on at 662 Locations in Puerto Rico During Island-Wide Blackout," *Electrek*, April 18, 2018, retrieved June 3, 2018, <https://electrek.co/2018/04/18/tesla-powerwall-powerpack-puerto-rico-blackout-elon-musk/>.
26. Richard Wolf, "Timeline: Same-Sex Marriage Through the Years," *USA Today*, June 24, 2015, retrieved June 3, 2018, <https://www.usatoday.com/story/news/politics/2015/06/24/same-sex-marriage-timeline/29173703/>.
27. Anastasia Pantsios, "Burlington, Vermont, Becomes First U.S. City to Run On 100% Renewable Electricity," *EcoWatch*, February 10, 2015, retrieved November 15, 2018, <https://www.ecowatch.com/burlington-vermont-becomes-first-u-s-city-to-run-on-100-renewable-elec-1882012101.html>.
28. "Vermont: State Profile and Energy Estimates," US Energy Information Administration, n.d., retrieved June 3, 2018, <https://www.eia.gov/state/?sid=VT>.
29. Lisa Rathke, "Vermont Reduces Incentives for Renewable Energy Program," *Associated Press*, May 4, 2018, retrieved November 15, 2018, <https://www.apnews.com/020a179d40b54c81b47b30cb14070870>.
30. "Totals and Averages: Vermont," US Climate Data, n.d., retrieved June 3, 2018, <https://www.usclimatedata.com/climate/vermont/united-states/3215>.
31. "State of Vermont: Energy Sector Risk Profile," US Department of Energy, 2015, retrieved June 3, 2018, [https://www.energy.gov/sites/prod/files/2015/06/f22/VT\\_Energy%20Sector%20Risk%20Profile.pdf](https://www.energy.gov/sites/prod/files/2015/06/f22/VT_Energy%20Sector%20Risk%20Profile.pdf).
32. "Historical Monthly Snowfall, Burlington, VT," National Weather Service, n.d., retrieved June 3, 2018, <https://www.weather.gov/btv/historicalSnow>.
33. Robert Walton, "Tesla, Green Mountain Power Roll Out \$15/Month BTM Battery Program," *Utility Dive*, May 16, 2017, retrieved June 3, 2018, <https://www.utilitydive.com/news/tesla-green-mountain-power-roll-out-15month-btm-battery-program/442783/>.
34. Fred Lambert, "Tesla Deployed a New Powerpack System in the UK," *Electrek*, April 26, 2018, retrieved December 11, 2018, <https://electrek.co/2018/04/26/tesla-power->

- pack-system-uk/.
35. Fred Lambert, "Tesla Is Installing Powerwalls and Solar Power on 50,000 Homes to Create Biggest Virtual Power Plant in the World," *Electrek*, February 4, 2018, retrieved June 3, 2018, <https://electrek.co/2018/02/04/tesla-powerwall-solar-virtual-power-plant/>; Fred Lambert, "Tesla Deploys Another Big 50 MWh Powerpack Project in Australia," *Electrek*, November 16, 2018, retrieved December 11, 2018, <https://electrek.co/2018/11/16/tesla-powerpack-project-australia-megapack/>.
  36. Timothy Seppala, "Tesla Powerwall Systems Help Some Hawaii Schools Beat the Heat," *Engadget*, February 26, 2018, retrieved June 3, 2018, <https://www.engadget.com/2018/02/26/hawaii-powerwall-school-air-conditioning/>; Fred Lambert, "Tesla Deployed over 300 Powerwalls in Hawaiian Schools to Cool Down Hot Classrooms," *Electrek*, February 23, 2018, retrieved December 11, 2018, <https://electrek.co/2018/02/23/tesla-powerwall-hawaii-school/>.
  37. Fred Lambert, "Tesla Deploys New Powerpack Project That Could Save Colorado Ratepayers \$1 Million Per Year," *Electrek*, October 14, 2018, retrieved December 11, 2018, <https://electrek.co/2018/10/14/tesla-powerpack-project-save-colorado-ratepayers/>.
  38. Simon Alvarez, "Tesla to Partner with NY Utility Company on Battery Storage System," *Teslarati*, February 15, 2018, retrieved December 11, 2018, <https://www.teslarati.com/tesla-con-edison-utility-new-york-powerpack-battery-system/>.
  39. "Utilities," Tesla, n.d., retrieved June 3, 2018, n.d., <https://www.tesla.com/utilities>.
  40. "Google X: Project Loon," n.d., retrieved May 11, 2018, <https://x.company/loon/>.
  41. "FCC Grants Experimental License for Project Loon in Puerto Rico," Federal Communications Commission, October 7, 2017, retrieved May 11, 2018, <https://www.fcc.gov/document/fcc-grants-experimental-license-project-loon-puerto-rico>.
  42. Katie Roof, "Google Parent Alphabet Looks to Restore Cell Service in Puerto Rico with Project Loon Balloons," *TechCrunch*, October 7, 2017, retrieved December 11, 2018, <https://techcrunch.com/2017/10/07/google-parent-alphabet-looks-to-restore-cell-service-in-puerto-rico-with-project-loon-balloons/>.
  43. Richard Lawler, "Project Loon's LTE balloons Are Floating over Puerto Rico," *Engadget*, October 20, 2017, retrieved November 15, 2017, [www.engadget.com/2017/10/20/project-loon-att-puerto-rico/](http://www.engadget.com/2017/10/20/project-loon-att-puerto-rico/).
  44. Alastair Westgarth, "Turning on Project Loon in Puerto Rico," *Loon* (blog), October 20, 2017, retrieved December 11, 2018, <https://medium.com/loon-for-all/turning-on-project-loon-in-puerto-rico-f3aa41ad2d7f>.
  45. Louis Matsakis, "What Would Really Happen If Russia Attacked Undersea Internet Cables?" *WIRED*, January 5, 2018, retrieved May 30, 2018, <https://www.wired.com/story/russia-undersea-internet-cables/>; Prachi Bhardwaj, "Fiber Optic Wires, Servers, and More Than 550,000 Miles of Underwater Cables," *Business Insider*, June 23, 2018, retrieved June 23, 2019, <https://www.businessinsider.com/how-internet-works-infrastructure-photos-2018-5>; Tyler Cooper, "Google and Other Tech Giants Are Quietly Buying Up the Most Important Part of the Internet," April 6, 2019, retrieved June 23, 2019, <https://venturebeat.com/2019/04/06/google-and-other-tech-giants-are-quietly-buying-up-the-most-important-part-of-the-internet/>.
  46. Alan Mauldin, "Frequently Asked Questions: Submarine Cables 101," *Telegeography* (blog), February 14, 2017, retrieved July 8, 2018, <https://blog.telegeography.com/frequently-asked-questions-about-undersea-submarine-cables>.
  47. Bobbie Johnson, "How One Clumsy Ship Cut Off the Web for 75 Million People," *Guardian*, February 1, 2008, retrieved May 30, 2018, <https://www.theguardian.com/business/2008/feb/01/internationalpersonalfinancebusiness.internet>.
  48. Alexandra Chang, "Why Undersea Internet Cables Are More Vulnerable Than You Think," *WIRED*, April 2, 2014, retrieved May 30, 2018, <https://www.wired.com/2013/04/how-vulnerable-are-undersea-internet-cables/>.
  49. Will Oremus, "The Global Internet Is Being Attacked by Sharks, Google Confirms," *Slate*, August 15, 2014, retrieved May 30, 2018, [http://www.slate.com/blogs/future\\_](http://www.slate.com/blogs/future_)

- tense/2014/08/15/shark\_attacks\_threaten\_google\_s\_undersea\_internet\_cables\_video.html.
50. Lydia Saad, "The '40-Hour' Workweek Is Actually Longer—by Seven Hours," Gallup, August 29, 2014, retrieved July 8, 2018, <https://news.gallup.com/poll/175286/hour-workweek-actually-longer-seven-hours.aspx>.
  51. "Average Hours Per Day Parents Spent Caring for and Helping Household Children as Their Main Activity," American Time Use Survey, Bureau of Labor Statistics, June 28, 2018, retrieved July 8, 2018, <https://www.bls.gov/charts/american-time-use/activity-by-parent.htm>.
  52. Jeffrey Jones, "In U.S., 40% Get Less Than Recommended Amount of Sleep," Gallup, December 19, 2013, retrieved July 8, 2018, <https://news.gallup.com/poll/166553/less-recommended-amount-sleep.aspx>.
  53. "Time Spent in Leisure and Sports Activities for the Civilian Population by Selected Characteristics, Averages Per Day, 2017 Annual Averages," American Time Use Survey, Bureau of Labor Statistics, June 28, 2018, retrieved July 8, 2018, <https://www.bls.gov/news.release/atus.t11a.htm>.
  54. Joan Engebretson, "iGR: Average Monthly Broadband Usage Is 190 Gigabytes Monthly Per Household," Telecompetitor, September 26, 2016, retrieved July 8, 2018, <https://www.telecompetitor.com/igr-average-monthly-broadband-usage-is-190-gigabytes-monthly-per-household/>.
  55. Alex Choros, "How Much Data Do You Really Need?" WhistleOut, March 26, 2018, retrieved July 8, 2018, <https://www.whistleout.com.au/Broadband/Guides/Broadband-Usage-Guide#per-activity-usage>.
  56. "Tech Giants Are Building Their Own Undersea Fibre-Optic Networks," *Economist*, October 7, 2017, retrieved July 8, 2018, <https://www.economist.com.ezproxy.cul.columbia.edu/business/2017/10/07/tech-giants-are-building-their-own-undersea-fibre-optic-networks>.
  57. Alan Mauldin, "A Complete List of Content Providers' Submarine Cable Holdings," *Telegeography* (blog), November 9, 2017, retrieved July 8, 2018, <https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list>.
  58. Jameson Zimmer, "Google Owns 63,605 Miles and 8.5% of Submarine Cables Worldwide," *Broadband Now*, September 12, 2018, retrieved December 11, 2018, <https://broadbandnow.com/report/google-content-providers-submarine-cable-ownership/>.
  59. "Locations," Google Cloud, n.d., retrieved July 8, 2018, <https://cloud.google.com/cdn/docs/locations>.
  60. Christina Farr, "Google Has Hired Geisinger's David Feinberg to Lead Its Health Strategy," CNBC, November 8, 2018, retrieved December 11, 2018, <https://www.cnbc.com/2018/11/08/google-hires-geisinger-ceo-david-feinberg-to-oversee-health.html>.
  61. Dieter Bohn, "Google Fit Is Getting Redesigned with New Health-Tracking Rings," *Verge*, August 21, 2018, retrieved December 11, 2018, <https://www.theverge.com/2018/8/21/17761768/google-fit-redesign-heart-points-aha-whowear-os-android>.
  62. Leo Kelion, "Google-Nest Merger Raises Privacy Issues," BBC News, February 8, 2018, retrieved December 11, 2018, <https://www.bbc.com/news/technology-42989073>.
  63. Anne-Marie Slaughter, "Three Responsibilities Every Government Has Towards Its Citizens," World Economic Forum, February 13, 2017, retrieved May 12, 2018, <https://www.weforum.org/agenda/2017/02/government-responsibility-to-citizens-anne-marie-slaughter/>.
  64. Central Intelligence Agency, "Roadways," *The World Factbook*, n.d., retrieved May 12, 2018, <https://www.cia.gov/library/publications/the-world-factbook/fields/2085.html>.
  65. David Brooks, "The Stem and the Flower," *New York Times*, December 2, 2013, retrieved May 12, 2018, <https://www.nytimes.com/2013/12/03/opinion/brooks-the-stem-and-the-flower.html>.
  66. World Bank, "Power Outages in Firms in a Typical Month (Number)," World Bank Enterprise Surveys 2006–2017, n.d., retrieved May 12, 2018, <https://data.worldbank.org/>

- indicator/IC.ELC.OUTG?end=2017&start=2017&view=map&year\_high\_desc=false.
67. "Global Terrorism Index 2017," Institute for Economics & Peace, n.d., retrieved May 12, 2018, <http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf>.
  68. This included the investing and research arms of their organizations as well as their founders. For instance, for Google, I also included Alphabet, X (formerly known as Google X), GV (formerly known as Google Ventures), as well as investments by co-founders Sergey Brin and Larry Page. For Microsoft, I also included Microsoft Research. For Amazon, I also included Jeff Bezos and Bezos Expeditions. For Tesla, I also included Elon Musk, SolarCity, SpaceX, and the Boring Company.
  69. Multiple pages at Crunchbase, retrieved May 16, 2018, <https://www.crunchbase.com/>.
  70. Jeff Desjardins, "The Jeff Bezos Empire in One Giant Chart," Visual Capitalist, January 11, 2019, retrieved June 23, 2019, <https://www.visualcapitalist.com/jeff-bezos-empire-chart/>.
  71. Brian Caulfield, "Planetary Resources Co-Founder Aims to Create Space 'Gold Rush,'" *Forbes*, April 25, 2012, retrieved April 17, 2018, [www.forbes.com/sites/briancaulfield/2012/04/20/planetary-resources-co-founder-aims-to-create-a-gold-rush-in-space/#1b0b3cc56b9b](http://www.forbes.com/sites/briancaulfield/2012/04/20/planetary-resources-co-founder-aims-to-create-a-gold-rush-in-space/#1b0b3cc56b9b).
  72. "What Are Rare Earths?," Rare Earth Technology Alliance, n.d., retrieved April 25, 2018, [www.rareearthtechalliance.com/What-are-Rare-Earths](http://www.rareearthtechalliance.com/What-are-Rare-Earths).
  73. H. Ali Saleem et al., "Mineral Supply for Sustainable Development Requires Resource Governance," *Nature* 543 (March 15, 2017): 367–72, retrieved May 30, 2018, <https://www.nature.com/articles/nature21359>.
  74. "Russian Deputy PM Sees No Reason for Competing with Musk on Launch Vehicles Market," TASS Russian News Agency, April 17, 2018, retrieved May 12, 2018, <http://tass.com/science/1000229>.
  75. "Origins of the Commercial Space Industry," Federal Aviation Administration, n.d., retrieved May 12, 2018, [https://www.faa.gov/about/history/milestones/media/Commercial\\_Space\\_Industry.pdf](https://www.faa.gov/about/history/milestones/media/Commercial_Space_Industry.pdf).
  76. "UCS Satellite Database," Union of Concerned Scientists, n.d., retrieved May 12, 2018, <https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.WvbCJM-dE5>.
  77. Steve Dent, "SpaceX Price Hikes Will Make ISS Cargo Missions More Costly," *Engadget*, April 27, 2018, retrieved May 12, 2018, <https://www.engadget.com/2018/04/27/spacex-price-hikes-iss-resupply-costs/>.
  78. Tim Fernholz, "Jeff Bezos Says He's Putting Billions into Space; He's Not Alone," *Quartz*, April 11, 2017, retrieved May 12, 2018, <https://qz.com/955427/jeff-bezos-says-hes-putting-billions-into-his-space-company-blue-origin-hes-not-alone/>.
  79. "Technology Grows Exponentially," Big Think, n.d., retrieved May 12, 2018, <http://bigthink.com/think-tank/big-idea-technology-grows-exponentially>.
  80. "Major Countries in Rare Earth Mine Production Worldwide from 2012 to 2017," Statista, n.d., retrieved May 12, 2018, [www.statista.com/statistics/268011/top-countries-in-rare-earth-mine-production/](http://www.statista.com/statistics/268011/top-countries-in-rare-earth-mine-production/).
  81. Mayuko Yatsu, "Revisiting Rare Earths: The Ongoing Efforts to Challenge China's Monopoly," *Diplomat*, August 29, 2017, retrieved May 30, 2018, <https://thediplomat.com/2017/08/revisiting-rare-earths-the-ongoing-efforts-to-challenge-chinas-monopoly/>.
  82. Charlotte McLeod, "Top Rare Earth Reserves by Country," *Rare Earth Investing News*, May 22, 2019, retrieved June 23, 2019, <https://investingnews.com/daily/resource-investing/critical-metals-investing/rare-earth-investing/rare-earth-reserves-country/>.
  83. Amber Pariona, "The Poles of Inaccessibility of Our Planet," *WorldAtlas*, August 5, 2016, retrieved May 12, 2018, [www.worldatlas.com/articles/the-poles-of-inaccessibility-of-our-planet.html](http://www.worldatlas.com/articles/the-poles-of-inaccessibility-of-our-planet.html); Andrew Higgins, "China's Ambitious New 'Port': Landlocked Kazakhstan," *New York Times*, January 1, 2018, retrieved May 12, 2018, [www.nytimes.com](http://www.nytimes.com).

- com/2018/01/01/world/asia/china-kazakhstan-silk-road.html.
84. Lazaro Gamio, "The Staggering Scale of China's Belt and Road Initiative," *Axios*, January 19, 2018, retrieved May 30, 2018, <https://www.axios.com/staggering-scale-china-infrastructure-142f3b1d-82b5-47b8-8ca9-57beb306f7df.html>.
  85. "Rare Earths: Battling China's Monopoly," *MINING*, September 16, 2011, retrieved May 12, 2018, [www.mining.com/rare-earths-battling-chinas-monopoly-after-molycorps-debacle/](http://www.mining.com/rare-earths-battling-chinas-monopoly-after-molycorps-debacle/).
  86. Charles Clover, "China's Xi Hails Belt and Road as 'Project of the Century,'" *Financial Times*, May 14, 2017, retrieved May 12, 2018, [www.ft.com/content/88d584a2-385e-11e7-821a-6027b8a20f23](http://www.ft.com/content/88d584a2-385e-11e7-821a-6027b8a20f23).
  87. Max Roser, "The World Is Much Better; The World Is Awful; The World Can Be Much Better," *Our World in Data* (blog), October 31, 2018, retrieved December 11, 2018, <https://ourworldindata.org/much-better-awful-can-be-better>.
  88. Fred Lambert, "Tesla Unveils 'First of Many Solar+Storage Projects' at Hospital in Puerto Rico," *Electrek*, October 24, 2019, retrieved December 11, 2018, <https://electrek.co/2017/10/24/tesla-unveils-first-solar-storage-projects-hospital-puerto-rico/>.
  89. J. J. Gallagher, "Struggling Puerto Rico Children's Hospital Gets Solar Power from Tesla," *ABC News*, October 25, 2017, retrieved December 11, 2018, <https://abcnews.go.com/US/struggling-puerto-rico-childrens-hospital-solar-power-tesla/story?id=50721869>.

### CHAPTER 3: PRIVACY ALLIES AND ADVERSARIES

1. Jonathan Stempel, "Lawsuit Says Google Tracks Phone Users Regardless of Privacy Settings," *Reuters*, August 20, 2018, retrieved September 12, 2018, <https://www.reuters.com/article/us-alphabet-google-privacy-lawsuit/lawsuit-says-google-tracks-phone-users-regardless-of-privacy-settings-idUSKCN1L51M3>.
2. "Patacsil v. Google, Inc.," Case No. 5:2018cv05062, Justia Legal Resources, Dockets & Filings, August 17, 2018, retrieved September 12, 2018, <https://dockets.justia.com/docket/california/candce/5:2018cv05062/330787>.
3. Ryan Nakashima, "'Location History' Off? Google's Still Tracking You," *Associated Press*, August 13, 2018, retrieved September 12, 2018, <https://apnews.com/828aefab64d4411bac257a07c1af0ecb>; "About CSE Security Services," CSE Security Services, n.d., retrieved September 12, 2018, <https://www.cseservices.net/about.html>.
4. "Class Action Complaint," case no. 18-5062, US District Court, Northern District of California, DocumentCloud, August 17, 2018, retrieved September 12, 2018, <https://www.documentcloud.org/documents/4777351-Gov-UScourts-Cand-330787-1-0.html>.
5. "AB-375 Privacy: Personal Information: Businesses," California Legislative Information, June 29, 2018, retrieved September 12, 2018, [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180AB375](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375).
6. Greg Ferenstein, "Google's Vint Cerf Says 'Privacy May Be an Anomaly.' Historically, He's Right," *TechCrunch*, November 20, 2013, retrieved August 12, 2018, <https://techcrunch.com/2013/11/20/googles-cerf-says-privacy-may-be-an-anomaly-historically-hes-right/>.
7. John Methven, "Why We Sleep Together," *Atlantic*, June 11, 2014, retrieved August 12, 2018, <https://www.theatlantic.com/health/archive/2014/06/why-we-sleep-together/371477/>.
8. Greg Ferenstein, "The Birth and Death of Privacy: 3,000 Years of History," *Medium*, November 25, 2015, retrieved August 12, 2018, <https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e>.
9. R. E. Behrman and M. J. Field, eds., *When Children Die: Improving Palliative and End-of-Life Care for Children and Their Families* (Washington, DC: National Academies Press, 2003).
10. John Whiting, *Culture and Human Development: The Selected Papers of John Whit-*

- ing, edited by Eleanor Hollenberg Chasdi (Cambridge, UK: Cambridge University Press, 2006).
11. "The Coercive Acts," Our American Revolution, n.d., retrieved August 12, 2018, <http://www.ouramericanrevolution.org/index.cfm/page/view/m0197>.
  12. Mark Kinsler, "The Luxury of a Private Telephone Line: 1939," *Lancaster Eagle Gazette*, August 3, 2014, retrieved August 12, 2018, <https://www.lancastereaglegazette.com/story/news/history/remember-when/2014/08/03/luxury-private-telephone-line/13547025/>.
  13. "The Rise of Mobile Phones: 20 Years of Global Adoption," *Cartesian* (blog), n.d., retrieved August 12, 2018, <https://blog.cartesian.com/the-rise-of-mobile-phones-20-years-of-global-adoption>.
  14. Jacob Kastrenakes, "Google's Chief Internet Evangelist Says 'Privacy May Actually Be an Anomaly,'" *Verge*, November 20, 2013, retrieved August 12, 2018, <https://www.theverge.com/2013/11/20/5125922/vint-cerf-google-internet-evangelist-says-privacy-may-be-anomaly>.
  15. "Employment by Industry 1910 and 2015," Bureau of Labor Statistics, n.d., retrieved August 12, 2018, <https://www.bls.gov/opub/ted/2016/employment-by-industry-1910-and-2015.htm>.
  16. Hilda Bastian, "The Hawthorne Effect: An Old Scientists' Tale Lingerin' in the Gunsmoke of Academic Snipers," *Absolutely Maybe* (blog), *Scientific American*, July 26, 2013, retrieved August 12, 2018, <https://blogs.scientificamerican.com/absolutely-maybe/the-hawthorne-effect-an-old-scientistse28099-tale-lingering-e2809cin-the-gunsmoke-of-academic-sniperse2809d/>.
  17. David Evans, "The Hawthorne Effect: What Do We Really Learn from Watching Teachers (and Others)?," *Development Impact* (blog), World Bank, February 17, 2014, retrieved August 12, 2018, <http://blogs.worldbank.org/impactevaluations/hawthorne-effect-what-do-we-really-learn-watching-teachers-and-others>.
  18. Sander van der Linden, "How the Illusion of Being Observed Can Make You a Better Person," *Scientific American*, November 3, 2011, retrieved August 12, 2018, <https://www.scientificamerican.com/article/how-the-illusion-of-being-observed-can-make-you-better-person/>; R. Oda, Y. Kato, and K. Hiraishi, "The Watching-Eye Effect on Prosocial Lying," *Evolutionary Psychology* 13, no. 3 (2015), <https://doi.org/10.1177/1474704915594959>.
  19. Padraig Flanagan, "Crime . . . the Answer's Staring You in the Face: The Striking New Police Poster That Has Slashed Thefts by Up to 40 Per Cent," *Daily Mail*, June 1, 2013, retrieved August 17, 2018, <http://www.dailymail.co.uk/news/article-2334577/Crime—answers-staring-face-The-striking-new-police-poster-slashed-thefts-40-cent.html>.
  20. Tom Stafford, "What Causes That Feeling of Being Watched?," *BBC News*, May 15, 2017, retrieved August 12, 2018, <http://www.bbc.com/future/story/20170512-what-causes-that-feeling-of-being-watched>.
  21. Daniel Levitin, "Why It's So Hard to Pay Attention, Explained by Science," *Fast Company*, September 23, 2015, retrieved August 12, 2018, <https://www.fastcompany.com/3051417/why-its-so-hard-to-pay-attention-explained-by-science>.
  22. Kimron Shapiro, ed., *The Limits of Attention: Temporal Constraints in Human Information Processing* (New York: Oxford Univ. Press, 2001).
  23. Tim Hornyak, "Fujitsu Supercomputer Simulates 1 Second of Brain Activity," *CNET*, August 5, 2013, retrieved August 17, 2018, <https://www.cnet.com/news/fujitsu-supercomputer-simulates-1-second-of-brain-activity/>.
  24. "Apple iMac 'Core i5' 2.8 21.5-Inch (Late 2015) Specs," *EveryMac*, n.d., retrieved August 17, 2018, <https://everymac.com/systems/apple/imac/specs/imac-core-i5-2.8-21-inch-aluminum-late-2015-specs.html>.
  25. Chris Smith, "Our Brains Might Hold 1 Petabyte of Data, Which Is Almost the Entire Internet," *BGR*, January 21, 2016, retrieved August 17, 2018, <https://bgr.com/2016/01/21/brain-memory-capacity-petabyte/>; Stephanie Pappas, "How Big Is the Internet, Re-

- ally?," *Live Science*, March 18, 2016, retrieved August 17, 2018, <https://www.livescience.com/54094-how-big-is-the-internet.html>.
26. "Vehicle Size Classes Used in the Fuel Economy Guide," US Department of Energy, n.d., retrieved August 17, 2018, <https://www.fueleconomy.gov/feg/info.shtml#sizeclasses>.
  27. Tripp Mickle, "Apple Unveils Ways to Help Limit iPhone Usage," *Wall Street Journal*, June 8, 2018, retrieved August 17, 2018, <https://www.wsj.com/articles/apple-unveils-ways-to-help-limit-iphone-usage-1528138570>.
  28. "Google Wants You to Get Off Your Phone Every Once in a While," *Wall Street Journal*, retrieved August 17, 2018, [https://www.wsj.com/articles/new-android-version-will-tell-users-how-long-they-have-been-on-various-apps-1525813268?mod=searchresults&page=1&pos=3&mod=article\\_inline](https://www.wsj.com/articles/new-android-version-will-tell-users-how-long-they-have-been-on-various-apps-1525813268?mod=searchresults&page=1&pos=3&mod=article_inline).
  29. Jacob Ward, "Why Data, Not Privacy, Is the Real Danger," NBC, February 4, 2019, retrieved February 5, 2019, <https://www.nbcnews.com/business/business-news/why-data-not-privacy-real-danger-n966621>.
  30. Issie Lapowsky, "Facebook Exposed 87 Million Users to Cambridge Analytica," *WIRED*, April 4, 2018, retrieved December 16, 2018, <https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/>.
  31. Will Oremus, "The Real Scandal Isn't What Cambridge Analytica Did," *Slate*, March 20, 2018, retrieved December 16, 2018, <https://slate.com/technology/2018/03/the-real-scandal-isnt-cambridge-analytica-its-facebooks-whole-business-model.html>.
  32. Ben Popken, "Congress Ratchets Up Pressure on Facebook, Twitter, Google," NBC News, November 1, 2017, retrieved December 16, 2018, <https://www.nbcnews.com/tech/tech-news/congress-ratchets-pressure-facebook-twitter-google-n816521>.
  33. Zach Wichter, "2 Days, 10 Hours, 600 Questions: What Happened When Mark Zuckerberg Went to Washington," *New York Times*, April 12, 2018, retrieved December 16, 2018, <https://www.nytimes.com/2018/04/12/technology/mark-zuckerberg-testimony.html>.
  34. Sean Burch, "'Senator, We Run Ads': Hatch Mocked for Basic Facebook Question to Zuckerberg," *SFGATE*, April 10, 2018, retrieved December 16, 2018, <https://www.sfgate.com/entertainment/the-wrap/article/Senator-We-Run-Ads-Hatch-Mocked-for-Basic-12822523.php>.
  35. Issie Lapowsky, "The Sundar Pichai Hearing Was a Major Missed Opportunity," *WIRED*, December 11, 2018, retrieved December 16, 2018, <https://www.wired.com/story/congress-sundar-pichai-google-ceo-hearing/>.
  36. Derek Hawkins, "The Cybersecurity 202: Why a Privacy Law Like GDPR Would Be a Tough Sell in the U.S.," *Washington Post*, May 25, 2018, retrieved September 12, 2018, [https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/?utm\\_term=.772dcf3c7ae2](https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/?utm_term=.772dcf3c7ae2).
  37. Ian Bogost, "Welcome to the Age of Privacy Nihilism," *Atlantic*, August 23, 2018, retrieved September 12, 2018, <https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198/>.
  38. Lee Raines, "Theme 3: Trust Will Not Grow, but Technology Usage Will Continue to Rise as a 'New Normal' Sets In," Pew Research Center: Internet and Technology, August 10, 2017, retrieved September 12, 2018, <http://www.pewinternet.org/2017/08/10/theme-3-trust-will-not-grow-but-technology-usage-will-continue-to-rise-as-a-new-normal-sets-in/>.
  39. J. Lau, B. Zimmerman, and F. Schaub, "Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers," *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW issue (2018): 102.
  40. Kaleigh Rogers, "People Who Buy Smart Speakers Have Given Up on Privacy, Researchers Find," *Vice Motherboard*, November 26, 2018, retrieved December 16, 2018, [https://motherboard.vice.com/en\\_us/article/vba7xj/people-who-buy-smart-speakers-have-given-up-on-privacy-researchers-find](https://motherboard.vice.com/en_us/article/vba7xj/people-who-buy-smart-speakers-have-given-up-on-privacy-researchers-find).

41. Bernard Marr, "Where Can You Buy Big Data? Here Are the Biggest Consumer Data Brokers," *Forbes*, September 7, 2017, retrieved December 16, 2018, <https://www.forbes.com/sites/bernardmarr/2017/09/07/where-can-you-buy-big-data-here-are-the-biggest-consumer-data-brokers/#3ea1f8556c27>.
42. Yael Grauer, "What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?," *Vice Motherboard*, March 27, 2018, retrieved June 6, 2018, [https://motherboard.vice.com/en\\_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection](https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection).
43. Nick Routley, "The Multi-Billion-Dollar Industry That Makes Its Living from Your Data," *Visual Capitalist*, April 14, 2018, retrieved June 6, 2018, <http://www.visualcapitalist.com/personal-data-ecosystem/>.
44. "Data Brokers: A Call for Transparency and Accountability," Federal Trade Commission, May 2014, retrieved June 8, 2018, <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>, p. 8.
45. "Media Advertising Spending in the United States from 2015 to 2021 (in Billion U.S. Dollars)," Statista, n.d., retrieved December 16, 2018, <https://www.statista.com/statistics/272314/advertising-spending-in-the-us/>.
46. "Terms of Use," Expedia, n.d., retrieved June 10, 2018, <https://www.expedia.com/p/info-other/legal.htm>.
47. "Terms and Conditions," Kayak, n.d., retrieved June 10, 2018, <https://www.kayak.com/terms-of-use>.
48. "Terms of Use Agreement," Match.com, n.d., retrieved June 10, 2018, <https://www.match.com/registration/membagr.aspx?lid=4>.
49. "Terms and Conditions," OkCupid, n.d., retrieved June 10, 2018, <https://www.okcupid.com/legal/terms>.
50. Julie Belluz, "Grindr Is Revealing Its Users' HIV Status to Third-Party Companies," *Vox*, April 3, 2018, retrieved June 6, 2018, <https://www.vox.com/2018/4/2/17189078/grindr-hiv-status-data-sharing-privacy>.
51. "FTC Recommends Congress Require the Data Broker Industry to Be More Transparent and Give Consumers Greater Control over Their Personal Information," Federal Trade Commission, May 27, 2014, retrieved December 16, 2018, <https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more>.
52. Craig Timberg, "Brokers Use 'Billions' of Data Points to Profile Americans," *Washington Post*, May 27, 2014, retrieved June 6, 2018, [https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19\\_story.html?utm\\_term=.c4b1dca54f3d](https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html?utm_term=.c4b1dca54f3d).
53. Julia Angwin, "Why Online Tracking Is Getting Creepier," *ProPublica*, June 12, 2014, retrieved June 6, 2018, <https://www.propublica.org/article/why-online-tracking-is-getting-creepier>.
54. Jeff Pollard, "Equifax Does More Than Credit Scores," *Forbes*, September 8, 2017, retrieved June 6, 2018, <https://www.forbes.com/sites/forrester/2017/09/08/equifax-does-more-than-credit-scores/#175a6ba119d8>.
55. Selena Larson, "The Hacks That Left Us Exposed in 2017," *CNN*, December 20, 2017, retrieved June 6, 2018, <http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html?iid=EL>.
56. Sarah Perez, "47.3 Million U.S. Adults Have Access to a Smart Speaker, Report Says," *TechCrunch*, March 7, 2018, retrieved June 6, 2018, <https://techcrunch.com/2018/03/07/47-3-million-u-s-adults-have-access-to-a-smart-speaker-report-says/>.
57. Kevin Murnane, "Amazon's Alexa Hacked to Surreptitiously Record Everything It Hears," *Forbes*, April 25, 2018, retrieved June 6, 2018, <https://www.forbes.com/sites/kevinmurnane/2018/04/25/amazons-alexa-hacked-to-surreptitiously-record-everything-it-hears/#549b96dc4fe2>.

58. Rob LeFebvre, "Amazon May Give Developers Your Private Alexa Transcripts," *Engadget*, July 12, 2017, retrieved June 6, 2018, <https://www.engadget.com/2017/07/12/amazon-developers-private-alexa-transcripts/>.
59. "Bill of Rights—Full Text," Bill of Rights Institute, n.d., retrieved June 6, 2018, <https://www.billofrightsinstitute.org/founding-documents/bill-of-rights/>.
60. "GDPR Key Changes," EUGDPR, n.d., retrieved June 6, 2018, <https://www.eugdpr.org/key-changes.html>.
61. Sarah Perez, "Report: Smartphone Owners Are Using 9 Apps Per Day, 30 Per Month," *TechCrunch*, May 4, 2017, retrieved June 10, 2018, <https://techcrunch.com/2017/05/04/report-smartphone-owners-are-using-9-apps-per-day-30-per-month/>.
62. "Article 51: Supervisory Authority," General Data Protection Regulation (website), n.d., retrieved June 6, 2018, <https://gdpr-info.eu/art-51-gdpr/>.
63. For a handy plain-language explanation of the GDPR, check out "GDPR Requirements in Plain English," *Varonis* (blog), retrieved June 6, 2018, <https://blog.varonis.com/gdpr-requirements-list-in-plain-english/>; "Controversial Topics," EUGDPR, n.d., retrieved June 6, 2018, <https://www.eugdpr.org/controversial-topics.html>.
64. Adam Satariono, "U.S. News Outlets Block European Readers over New Privacy Rules," *New York Times*, May 25, 2018, retrieved June 6, 2018, <https://www.nytimes.com/2018/05/25/business/media/europe-privacy-gdpr-us.html>.
65. Emma Kidwell, "Ragnorak Online Shutting Down European Servers After 14 Years," *Gamasutra*, April 25, 2018, retrieved June 23, 2019, [https://www.gamasutra.com/view/news/317050/Ragnarok\\_Online\\_shutting\\_down\\_European\\_servers\\_after\\_14\\_years.php](https://www.gamasutra.com/view/news/317050/Ragnarok_Online_shutting_down_European_servers_after_14_years.php); Natasha Lomas, "Unroll.me to Close to EU Users Saying It Can't Comply with GDPR," *TechCrunch*, May 5, 2018, retrieved June 10, 2018, <https://techcrunch.com/2018/05/05/unroll-me-to-close-to-eu-users-saying-it-cant-comply-with-gdpr/>.
66. Alex Hern, "Facebook Moves 1.5bn Users out of Reach of New European Privacy Law," *Guardian*, April 19, 2018, retrieved June 6, 2018, <https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law>.
67. "Privacy Act of 1974," US Department of Justice, n.d., retrieved September 13, 2018, <https://www.justice.gov/opcl/privacy-act-1974>.
68. "5 U.S. Code §552a: Records Maintained on Individuals," Legal Information Institute, Cornell Law Library, n.d., retrieved June 6, 2018, <https://www.law.cornell.edu/uscode/text/5/552a>.
69. Julie Brill, "Millions Use Microsoft's GDPR Privacy Tools to Control Their Data—including 2 Million Americans," *Microsoft on the Issues* (blog), September 17, 2018, retrieved September 30, 2018, <https://blogs.microsoft.com/on-the-issues/2018/09/17/millions-use-microsofts-gdpr-privacy-tools-to-control-their-data-including-2-million-americans/>.
70. Elias Biryabarema, "Uganda Imposes Tax on Social Media Use," *Reuters*, May 31, 2018, retrieved June 6, 2018, <https://www.reuters.com/article/us-uganda-internet/uganda-imposes-tax-on-social-media-use-idUSKCN1IW2IK>.
71. Tara Francis Chan, "A South Pacific Nation Is Banning Facebook for a Month as the Region Grapples with Fake News and Censorship," *Business Insider*, May 29, 2018, retrieved June 6, 2018, <http://www.businessinsider.com/papua-new-guinea-will-temporarily-ban-facebook-2018-5>.
72. Rosie Perper, "After Declaring a State of Emergency, Sri Lanka Has Banned Facebook, Instagram, and WhatsApp," *Business Insider*, March 7, 2018, retrieved June 6, 2018, <http://www.businessinsider.com/sri-lanka-bans-facebook-to-stop-violence-2018-3>.
73. Rich Miller, "Google Gets Patent for Data Center Barges," *Data Center Knowledge*, April 29, 2009, retrieved June 6, 2018, [www.datacenterknowledge.com/archives/2009/04/29/google-gets-patent-for-data-center-barges](http://www.datacenterknowledge.com/archives/2009/04/29/google-gets-patent-for-data-center-barges).
74. Arman Shehabi et al., "United States Data Center Energy Usage Report," Ernest Orlando Lawrence Berkeley National Laboratory, June 2016, retrieved June 6, 2018, <http://eta->

- publications.lbl.gov/sites/default/files/lbnl-1005775\_v2.pdf.
75. Christopher Helman, "Berkeley Lab: It Takes 70 Billion Kilowatt Hours a Year to Run the Internet," *Forbes*, June 28, 2016, retrieved June 6, 2018, <https://www.forbes.com/sites/christopherhelman/2016/06/28/how-much-electricity-does-it-take-to-run-the-internet/#202ebfe91fff>.
  76. "Nordic Data Center Construction Market: Industry Outlook and Forecast 2018–2023," Research and Markets, Business Wire, May 23, 2018, retrieved June 6, 2018, <https://www.businesswire.com/news/home/20180523006288/en/Nordic-Data-Center-Construction-Market-Industry>.
  77. "Microsoft Plumbs Ocean's Depths to Test Underwater Data Center," *New York Times*, January 31, 2016, retrieved June 6, 2018, [https://www.nytimes.com/2016/02/01/technology/microsoft-plumbs-oceans-depths-to-test-underwater-data-center.html?\\_r=0](https://www.nytimes.com/2016/02/01/technology/microsoft-plumbs-oceans-depths-to-test-underwater-data-center.html?_r=0).
  78. "How Much Water Is in the Ocean?" National Oceanic and Atmospheric Administration, n.d., retrieved June 6, 2018, <https://oceanservice.noaa.gov/facts/oceanwater.html>.
  79. "Project Natick," Microsoft, retrieved June 6, 2018, <http://natick.research.microsoft.com/>.

#### CHAPTER 4: INFORMATION-AGE WARFIGHTERS

1. "Captured ISIS Fighter on How He Was Betrayed," YouTube, October 23, 2014, retrieved January 11, 2019, [https://www.youtube.com/watch?v=mtj3M\\_Bb0z8&list=PL0l4bTGBHlMEAgZoMlCEKD5TzKWOEYAdJ&index=2&internalcountrycode=AE](https://www.youtube.com/watch?v=mtj3M_Bb0z8&list=PL0l4bTGBHlMEAgZoMlCEKD5TzKWOEYAdJ&index=2&internalcountrycode=AE).
2. "The Redirect Method: A Blueprint for Bypassing Extremism," Google Jigsaw, n.d., retrieved May 11, 2018, <https://redirectmethod.org/downloads/RedirectMethod-Full-Method-PDF.pdf>, p. 4.
3. J. Uchill, "Exclusive: 'Redirecting' Extremists Away from Radical Content," Axios, March 28, 2018, retrieved May 11, 2018, <https://www.axios.com/redirecting-extremists-away-from-radical-content-352b74e7-a3e0-4e21-9253-40a95089aa9c.html>.
4. J. Uchill, "Exclusive: 'Redirecting' Extremists Away from Radical Content," Axios, March 28, 2018, retrieved May 11, 2018, <https://www.axios.com/redirecting-extremists-away-from-radical-content-352b74e7-a3e0-4e21-9253-40a95089aa9c.html>.
5. "The Redirect Method: A Blueprint for Bypassing Extremism," Google Jigsaw, n.d., retrieved May 11, 2018, <https://redirectmethod.org/downloads/RedirectMethod-Full-Method-PDF.pdf>, p.13; note that total of videos played breaks down to 347,195 minutes in Arabic and 152,875 minutes in English.
6. J. Uchill, "Exclusive: 'Redirecting' Extremists Away from Radical Content," Axios, March 28, 2018, retrieved May 11, 2018, <https://www.axios.com/redirecting-extremists-away-from-radical-content-352b74e7-a3e0-4e21-9253-40a95089aa9c.html>.
7. Charles Bagli, "\$2.4 Billion Deal for Chelsea Market Enlarges Google's New York Footprint," *New York Times*, February 7, 2018, retrieved January 11, 2019, <https://www.nytimes.com/2018/02/07/nyregion/google-chelsea-market-new-york.html>.
8. Eric Schmidt, "Google Ideas Becomes Jigsaw," Medium, February 16, 2016, retrieved May 11, 2018, <https://medium.com/jigsaw/google-ideas-becomes-jigsaw-bcb5bd08c423#.oi1ydhk9m>.
9. "Total Number of Websites," Internet Live Stats, n.d., retrieved July 20, 2018, <http://www.internetlivestats.com/total-number-of-websites/>.
10. Kimberly Hutcherson, "Six Days After a Ransomware Cyberattack, Atlanta Officials Are Filling Out Forms by Hand," CNN, March 28, 2018, retrieved November 20, 2018, <https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html>.
11. Jon Fingas, "Atlanta Ransomware Attack May Cost Another \$9.5 Million to Fix," Engadget, June 6, 2018, retrieved November 20, 2018, <https://www.engadget.com/2018/06/06/atlanta-ransomware-attack-struck-mission-critical-services/>.
12. David Allison, "City of Atlanta Paid 8 Firms \$2.7M to Combat Ransomware Attack,"

- Atlanta Business Chronicle*, April 24, 2018, retrieved November 20, 2018, <https://www.bizjournals.com/atlanta/news/2018/04/24/city-of-atlanta-paid-8-firms-2-7m-to-combat.html>.
13. Larry Greenemeier, "Urban Bungle: Atlanta Cyber Attack Puts Other Cities on Notice," *Scientific American*, April 4, 2018, retrieved November 20, 2018, <https://www.scientificamerican.com/article/urban-bungle-atlanta-cyber-attack-puts-other-cities-on-notice/>.
  14. "The Tactics & Tropes of the Internet Research Agency," New Knowledge, December 17, 2018, retrieved January 13, 2019, <https://www.newknowledge.com/disinfo-report>.
  15. Alexis Wichowski, "Net States Rule the World: Ignore Them at Your Peril," *WIRED*, November 4, 2017, retrieved July 20, 2018, <https://www.wired.com/story/net-states-rule-the-world-we-need-to-recognize-their-power/>.
  16. Eric Schmitt, "In Battle to Defang ISIS, U.S. Targets Its Psychology," *New York Times*, December 28, 2014, [www.nytimes.com/2014/12/29/us/politics/in-battle-to-defang-isis-us-targets-its-psychology-.html?\\_r=0](http://www.nytimes.com/2014/12/29/us/politics/in-battle-to-defang-isis-us-targets-its-psychology-.html?_r=0).
  17. Renard Sexton, "Analysis: Did U.S. Aid Win Hearts and Minds in Afghanistan? Yes and No," *Washington Post*, January 6, 2017, [www.washingtonpost.com/news/monkey-cage/wp/2017/01/06/did-u-s-nonmilitary-aid-win-hearts-and-minds-in-afghanistan-yes-and-no/](http://www.washingtonpost.com/news/monkey-cage/wp/2017/01/06/did-u-s-nonmilitary-aid-win-hearts-and-minds-in-afghanistan-yes-and-no/).
  18. "How Extremists and Terror Groups Hijacked Social Media," BBC News, December 13, 2017, retrieved June 10, 2018, <https://www.bbc.co.uk/bbcthree/article/16b6c718-17d4-426d-add4-625af822e8d2>.
  19. Martin Evans, "Facebook Accused of Introducing Extremists to One Another Through 'Suggested Friends' Feature," *Telegraph*, May 5, 2018, retrieved June 10, 2018, <https://www.telegraph.co.uk/news/2018/05/05/facebook-accused-introducing-extremists-one-another-suggested/>.
  20. Natasha Bernal, "WhatsApp Admits Encryption Has Helped Criminals as It Plans Crackdown on Illegal Behaviour," *Telegraph*, July 4, 2018, retrieved July 20, 2018, <https://www.telegraph.co.uk/technology/2018/07/04/whatsapp-admits-encryption-has-helped-criminals-plans-crackdown/>.
  21. Andrew Russell, "'Rough Consensus and Running Code' and the Internet-OSI Standards War," *IEEE Annals of the History of Computing* 28, no. 3 (2006): 48–61.
  22. Philip Tetlock, *Expert Political Judgment: How Good Is It? How Can We Know?* (Princeton, NJ: Princeton Univ. Press, 2006).
  23. Stewart Brand, "Philip Tetlock," Long Now Foundation, n.d., retrieved June 10, 2018, [www.longnow.org/seminars/02007/jan/26/why-foxes-are-better-forecasters-than-hedgehogs/](http://www.longnow.org/seminars/02007/jan/26/why-foxes-are-better-forecasters-than-hedgehogs/).
  24. "Philip E. Tetlock," School of Arts and Sciences, University of Pennsylvania, n.d., retrieved June 10, 2018, <https://www.sas.upenn.edu/tetlock/bio>.
  25. Stewart Brand, "Philip Tetlock," Long Now Foundation, n.d., retrieved June 20, 2018, [www.longnow.org/seminars/02007/jan/26/why-foxes-are-better-forecasters-than-hedgehogs/](http://www.longnow.org/seminars/02007/jan/26/why-foxes-are-better-forecasters-than-hedgehogs/).
  26. "The Good Judgment Project," IARPA "Be the Future," n.d., retrieved June 20, 2018, [www.iarpa.gov/index.php/newsroom/iarpa-in-the-news/2015/439-the-good-judgment-project](http://www.iarpa.gov/index.php/newsroom/iarpa-in-the-news/2015/439-the-good-judgment-project).
  27. Tara Isabella Burton, "Future: Could You Be a 'Super-Forecaster'?", BBC, January 20, 2015, retrieved June 20, 2018, [www.bbc.com/future/story/20150120-are-you-a-super-forecaster](http://www.bbc.com/future/story/20150120-are-you-a-super-forecaster).
  28. "From Theory to Practice," Good Judgment, n.d., retrieved June 20, 2018, <https://good-judgment.com/ourStory.html>.
  29. Matthew Burton, "So You Want to Be an Intelligence Analyst," *MatthewBurton.org*, October 10, 2013, retrieved June 10, 2018, <http://matthewburton.org/become-an-intelligence-analyst/>.
  30. Leo Shane, "Up-or-Out Rules Get New Scrutiny from Congress," *Military Times*,

- January 25, 2018, retrieved June 10, 2018, <https://www.militarytimes.com/news/pentagon-congress/2018/01/25/congress-again-weighing-changes-to-militarys-officer-promotion-rules/>.
31. Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Penguin Books, 2015).
  32. Stanley McChrystal, "How the Military Can Teach Us to Adapt." *TIME*, June 9, 2015, retrieved July 2, 2019, <https://time.com/3904177/mcchrystal-team-of-teams/>.
  33. Robert Cross and Andrew Parker, *The Hidden Power of Social Networks: Understanding How Work Really Gets Done* (Brighton, MA: Harvard Business Review Press, 2004).
  34. Malcolm Gladwell, "On Connectors, Mavens, and Salesmen: How New Ideas Spread Like Seeds," *Fast Company*, July 30, 2012, [www.fastcompany.com/1799410/connectors-mavens-and-salesmen-how-new-ideas-spread-seeds](http://www.fastcompany.com/1799410/connectors-mavens-and-salesmen-how-new-ideas-spread-seeds).
  35. Chris Fussell, *One Mission: How Leaders Build a Team of Teams* (New York: Penguin Books, 2017).
  36. Ilan Mochari, "How General McChrystal's Share-and-Care Meetings Changed a Siloed Culture," *Inc.*, May 15, 2015, retrieved January 13, 2019, <https://www.inc.com/ilan-mochari/genearl-mcchrystal-meetings.html>.
  37. "Trident Juncture 2018," NATO, n.d., retrieved January 13, 2019, <https://www.nato.int/cps/en/natohq/157833.htm#glance>.
  38. Anders Fjellestad, "Cold Knowledge Is Hot in NATO," *Forsvaret*, April 18, 2018, retrieved January 13, 2019, <https://forsvaret.no/en/newsroom/news-stories/cold-knowledge-is-hot-in-nato>.
  39. Gerard O'Dwyer, "Finland, Norway Press Russia on Suspected GPS Jamming During NATO Drill," *Defense News*, November 16, 2018, retrieved January 13, 2019, <https://www.defensenews.com/global/europe/2018/11/16/finland-norway-press-russia-on-suspected-gps-jamming-during-nato-drill/>.
  40. "Traffic Statistics," Avinor, n.d., retrieved January 13, 2019, [https://avinor.no/en/corporate/airport/oslo/about-us/traffic\\_statistics/trafikkstatistikk](https://avinor.no/en/corporate/airport/oslo/about-us/traffic_statistics/trafikkstatistikk).
  41. Ryan Browne, "Russia Jammed GPS During Major NATO Military Exercise with US Troops," *CNN*, November 14, 2018, retrieved January 13, 2019, <https://edition.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html>.
  42. Courtney Kube, "Russia Has Figured Out How to Jam U.S. Drones in Syria, Officials Say," *NBC News*, April 10, 2018, retrieved January 13, 2019, <https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931>.
  43. Walker D. Mills, "Dear Google, Please Help Your Country Defend Itself," *Defense News*, January 27, 2019, retrieved February 4, 2019, <https://www.defensenews.com/smr/cultural-clash/2019/01/28/dear-google-please-help-your-country-defend-itself/>.
  44. "Army Futures Command," n.d., retrieved January 13, 2019, <https://www.army.mil/futures#org-about>.
  45. David Vergun, "Army Network Modernization Efforts Spearheaded by New Cross-Functional Teams," *Army News Service*, March 21, 2018, retrieved January 13, 2019, [https://www.army.mil/article/202500/army\\_network\\_modernization\\_efforts\\_spearheaded\\_by\\_new\\_cross\\_functional\\_teams](https://www.army.mil/article/202500/army_network_modernization_efforts_spearheaded_by_new_cross_functional_teams).
  46. Alyssa Goard, "Department of Defense, Army Futures Invest in Austin Hackathon Ideas," *KXAN News*, September 30, 2018, retrieved January 13, 2019, <https://www.kxan.com/news/local/austin/departement-of-defense-army-futures-invest-in-austin-hackathon-ideas/1488776718>.
  47. "U.S. Navy Brings Back Navigation by the Stars for Officers," *NPR*, February 22, 2016, retrieved January 13, 2019, <https://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers>.
  48. Julian Borger, "Trump Urges World to Reject Globalism in UN Speech That Draws Mocking Laughter," *Guardian*, September 26, 2018, retrieved September 27, 2018, <https://www.theguardian.com/us-news/2018/sep/25/trump-united-nations-general-assembly-speech-globalism-america>.

49. "Protecting Users and Customers Everywhere," Cybersecurity Tech Accord, n.d., retrieved June 23, 2018, <https://cybertechaccord.org/accord/>.
50. Brad Smith, "The Need for a Digital Geneva Convention," *Microsoft on the Issues* (blog), February 14, 2017, retrieved June 23, 2019, <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.
51. Press releases from the Office of Press Relations, US Department of State, n.d., retrieved July 15, 2018, <https://www.state.gov/r/pa/prs/index.htm>.
52. Ian Sherr, "Facebook, Apple, Microsoft and More Tech Companies Are Condemning Trump," CNET, June 26, 2018, retrieved July 15, 2018, <https://www.cnet.com/news/facebook-apple-microsoft-and-more-tech-companies-are-condemning-trump/>.
53. Ian Sherr, "Apple, Google, Facebook, and More Speak Out on DACA," CNET, September 6, 2017, retrieved July 15, 2018, <https://www.cnet.com/news/tech-has-its-say-about-president-trump-and-dreamers-daca-microsoft-zuckerberg/>.
54. Patrick Cockburn, "Preview 2018: After a String of Defeats in Iraq and Syria What 2018 Means for ISIS," *Independent*, January 1, 2018, retrieved July 20, 2018, <https://www.independent.co.uk/news/world/middle-east/isis-defeat-syria-latest-iraq-2018-survive-a8107891.html>.
55. Jason Burke, "Rise and Fall of ISIS: Its Dream of a Caliphate Is Over, So What Now?," *Guardian*, October 21, 2017, retrieved July 20, 2018, <https://www.theguardian.com/world/2017/oct/21/isis-caliphate-islamic-state-raqa-iraq-islamist>.
56. Jim Sciutto, "ISIS Can 'Muster' Between 20,000 and 31,500 Fighters, CIA Says," *CNN*, September 12, 2014, retrieved July 20, 2018, <https://www.cnn.com/2014/09/11/world/meast/isis-syria-iraq/index.html>.
57. Tim Lister et al., "ISIS Goes Global: 143 Attacks in 29 Countries Have Killed 2,043," *CNN*, February 12, 2018, retrieved July 20, 2018, <https://www.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world/index.html>.
58. "Foreign Terrorist Organizations," US Department of State, n.d., retrieved July 20, 2018, <https://www.state.gov/j/ct/rls/other/des/123085.htm>.
59. Katie Worth, "Lone Wolf Attacks Are Becoming More Common—And More Deadly," *PBS*, July 14, 2016, retrieved July 20, 2018, <https://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/>.
60. "Mass shooting" is defined by the Gun Violence Archive as an incident in which four or more people are shot, not including the shooter. "Mass Shootings in 2018," Gun Violence Archive, n.d., retrieved August 5, 2018, <http://www.gunviolencearchive.org/reports/mass-shooting>.
61. Amy Cohen et al., "Rate of Mass Shootings Has Tripled Since 2011, Harvard Research Shows," *Mother Jones*, October 11, 2014, retrieved July 20, 2018, <https://www.motherjones.com/politics/2014/10/mass-shootings-increasing-harvard-research/>.
62. Sherry Towers et al., "Contagion in Mass Killings and School Shootings," *PLoS One* 10, no. 7 (2015): e0117259.
63. "'Media Contagion' Is Factor in Mass Shootings, Study Says," press release from the American Psychological Association, August 4, 2016, retrieved July 20, 2018, <http://www.apa.org/news/press/releases/2016/08/media-contagion.aspx>.
64. "Mass Shootings in 2019," Gun Violence Archive, n.d., retrieved June 23, 2019, <https://www.gunviolencearchive.org/reports/mass-shooting>.
65. "'Media Contagion' Is Factor in Mass Shootings, Study Says," press release from the American Psychological Association, August 4, 2016, retrieved June 23, 2019, <http://www.apa.org/news/press/releases/2016/08/media-contagion.aspx>.
66. Christal Hayes, "After Florida Shooting, More Than 600 Copycat Threats Have Targeted Schools," *USA Today*, March 7, 2018, retrieved July 20, 2018, <https://www.usatoday.com/story/news/2018/03/07/within-nine-days-after-florida-shooting-there-were-more-than-100-threats-schools-across-u-s-its-not/359986002/>.
67. Kevin Drum, "How Many Threats Can the FBI Evaluate on a Daily Basis?," *Mother Jones*, February 18, 2018, retrieved July 20, 2018, <https://www.motherjones.com/kevin>

drum/2018/02/how-many-threats-can-the-fbi-evaluate-on-a-daily-basis/.

## CHAPTER 5: A GREAT WALL OF WATCHERS

1. Shannon Liao, "Google Admits It Tracked User Location Data Even When the Setting Was Turned Off," *Verge*, November 21, 2017, [www.theverge.com/2017/11/21/16684818/google-location-tracking-cell-tower-data-android-os-firebase-privacy](http://www.theverge.com/2017/11/21/16684818/google-location-tracking-cell-tower-data-android-os-firebase-privacy).
2. "State Council Notice Concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014–2020)," China Copyright & Media, June 24, 2014, retrieved June 20, 2018, <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014–2020/>.
3. "Millions in China with Bad 'Social Credit' Barred from Buying Plane, Train Tickets," Channel News Asia, March 16, 2018, retrieved June 20, 2018, <https://www.channelnewsasia.com/news/asia/china-bad-social-credit-barred-from-buying-train-plane-tickets-10050390>.
4. Maya Wang, "China's Chilling 'Social Credit' Blacklist," Human Rights Watch, December 12, 2017, retrieved June 20, 2018, <https://www.hrw.org/news/2017/12/12/chinas-chilling-social-credit-blacklist>.
5. Rachel Botsman, "Big Data Meets Big Brother as China Moves to Rate Its Citizens," *WIRED*, October 21, 2017, retrieved June 20, 2018, <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>.
6. "Opinions Concerning Accelerating the Construction of Credit Supervision, Warning and Punishment Mechanisms for Persons Subject to Enforcement for Trust-Breaking," China Copyright & Media, September 25, 2016, retrieved June 20, 2018, <https://chinacopyrightandmedia.wordpress.com/2016/09/25/opinions-concerning-accelerating-the-construction-of-credit-supervision-warning-and-punishment-mechanisms-for-persons-subject-to-enforcement-for-trust-breaking/>.
7. Yuan Yang, "China Penalises 6.7m Debtors with Travel Ban," *Financial Times*, February 15, 2017, retrieved July 5, 2018, <https://www.ft.com/content/ceb2a7f0-f350-11e6-8758-6876151821a6>.
8. Celia Hatton, "China 'Social Credit': Beijing Sets Up Huge System," BBC News, October 26, 2015, retrieved June 20, 2018, <https://www.bbc.com/news/world-asia-china-34592186>.
9. Simina Mistreanu, "Life Inside China's Social Credit Laboratory," *Foreign Policy*, April 3, 2018, retrieved June 20, 2018, <http://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/>.
10. "What's Your Citizen 'Trust Score'? China Moves to Rate Its 1.3 Billion Citizens," WUNC Public Radio, November 10, 2017, retrieved June 20, 2018, <http://wunc.org/post/whats-your-citizen-trust-score-china-moves-rate-its-13-billion-citizens#stream/0>.
11. Leslie Holmes, *Communism: A Very Short Introduction* (New York: Oxford University Press, 2009), 9.
12. "China Pulls Further Ahead of US in Mobile Payments with Record US\$12.8 Trillion in Transactions," *South China Morning Post*, February 20, 2018, retrieved July 5, 2018, <https://www.scmp.com/tech/apps-gaming/article/2134011/china-pulls-further-ahead-us-mobile-payments-record-us128-trillion>.
13. Cheang Ming, "FICO with Chinese Characteristics: Nice Rewards, but Punishing Penalties," CNBC, March 16, 2017, retrieved July 5, 2018, <https://www.cnbc.com/2017/03/16/china-social-credit-system-ant-financials-sesame-credit-and-others-give-scores-that-go-beyond-fico.html>.
14. Ann Carrns, "For Those in Their 20s, a Finding That They Don't Manage Debt Well," *New York Times*, November 20, 2013, retrieved July 5, 2018, <https://www.nytimes.com/2013/11/20/business/for-those-in-their-20s-a-finding-that-they-dont-manage-debt-well.html>.
15. "Planning Outline for the Construction of a Social Credit System (2014–2020)," China

- Copyright & Media, June 14, 2014, retrieved July 5, 2018, <https://chinacopyrightand-media.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>.
16. Mara Hvistendhal, "Inside China's Vast New Experiment in Social Ranking," *WIRED*, December 14, 2017, retrieved July 5, 2018, <https://www.wired.com/story/age-of-social-credit>.
  17. Jonathan Margolis, "A Big Brother Approach Has Qualities That Would Benefit Society," *Financial Times*, October 31, 2017, retrieved July 5, 2018, <https://www.ft.com/content/ffe78e52-bd54-11e7-823b-ed31693349d3>.
  18. M. J. Franklin, "'People You May Know' Is the Perfect Demonstration of Everything That's Wrong with Facebook," Yahoo News, May 15, 2018, retrieved February 4, 2019, <https://finance.yahoo.com/news/apos-people-may-know-apos-142239841.html>.
  19. Endnote TK.
  20. Russell Brandom, "Shadow Profiles Are the Biggest Flaw in Facebook's Privacy Defense," *Verge*, April 11, 2018, retrieved June 27, 2019, <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy>.
  21. Violet Blue, "Firm: Facebook's Shadow Profiles Are 'Frightening' Dossiers on Everyone," *ZDNet*, June 24, 2013, retrieved February 4, 2019, <https://www.zdnet.com/article/firm-facebooks-shadow-profiles-are-frightening-dossiers-on-everyone/>.
  22. Jessica Guynn, "Bye Facebook, Hello Instagram: Users Make Beeline for Facebook-Owned Social Network," *USA Today*, March 22, 2018, retrieved February 4, 2019, <https://www.usatoday.com/story/tech/news/2018/03/22/bye-facebook-hello-instagram-users-make-beeline-facebook-owned-social-network/433361002/>.
  23. Steven Musil, "Facebook 'Unintentionally Uploaded' Email Contacts from 1.5M Users," *CNET*, April 17, 2019, retrieved June 27, 2019, <https://www.cnet.com/news/facebook-unintentionally-uploaded-email-contacts-from-1-5m-users/>.
  24. Leo Mirani, "Millions of Facebook users have no idea they're using the internet," *Quartz*, February 9, 2015, retrieved June 27, 2019, <https://qz.com/333313/millions-of-facebook-users-have-no-idea-theyre-using-the-internet/>.
  25. Sam Weber, "How Online Social Movements Translate to Offline Results," *PBS NewsHour*, June 10, 2017, retrieved June 27, 2019, <https://www.pbs.org/newshour/show/online-social-movements-translate-offline-results>.
  26. "More than 12M 'Me Too' Facebook Posts, Comments, Reactions in 24 Hours," *CBS News*, October 17, 2017, retrieved June 27, 2019, <https://www.cbsnews.com/news/metoo-more-than-12-million-facebook-posts-comments-reactions-24-hours/>.
  27. Issie Lapowsky, "For Philando Castile, Social Media Was the Only 911," *WIRED*, July 7, 2016, retrieved June 27, 2019, <https://www.wired.com/2016/07/philando-castile-social-media-911/>.
  28. Jessi Hempel, "Social Media Made the Arab Spring, But It Couldn't Save It," *WIRED*, January 26, 2016, retrieved June 27, 2019, <https://www.wired.com/2016/01/social-media-made-the-arab-spring-but-couldnt-save-it/>.
  29. "Nearly Half of Americans Get News Through Facebook," *Pew Research Center: Fact Tank*, April 9, 2018, retrieved June 27, 2019, [https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook/ft\\_18-04-06\\_facebooknews/](https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook/ft_18-04-06_facebooknews/).
  30. Li Tao, "Jaywalkers Under Surveillance in Shenzhen Soon to Be Punished via Text Messages," *South China Morning Post*, March 27, 2018, retrieved June 20, 2018, <http://www.scmp.com/tech/china-tech/article/2138960/jaywalkers-under-surveillance-shenzhen-soon-be-punished-text>.
  31. Tara Chan, "22 Eerie Photos Show How China Uses Facial Recognition to Track Its Citizens as They Travel, Shop—and Even Use Toilet Paper," *Business Insider*, February 12, 2018, retrieved June 20, 2018, <http://www.businessinsider.com/how-china-uses-facial-recognition-technology-surveillance-2018-2#customers-of-china-merchants-bank-scan-their-faces-instead-of-their-bank-cards-at-some-1000-atms-users-still-need-to-enter-a-pin-though-11>.

32. "Facial Recognition Surveillance Test Extended at Berlin Train Station," *Deutsche Welle*, December 15, 2017, retrieved June 20, 2018, <http://www.dw.com/en/facial-recognition-surveillance-test-extended-at-berlin-train-station/a-41813861>.
33. Lynsey Chutel, "China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database," *Quartz*, May 25, 2018, retrieved June 20, 2018, <https://qz.com/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/>.
34. Paul Mozur, "Inside China's Big Tech Conference, New Ways to Track Citizens," *New York Times*, December 5, 2017, retrieved June 20, 2018, <https://www.nytimes.com/2017/12/05/business/china-internet-conference-wuzhen.html>.
35. "Backing Big Brother: Chinese Facial Recognition Firms Appeal to Funds," *Reuters*, November 12, 2017, retrieved June 20, 2018, <https://www.reuters.com/article/us-china-facialrecognition-analysis/backing-big-brother-chinese-facial-recognition-firms-appeal-to-funds-idUSKBN1DD00A>.
36. "SenseTime," *Crunchbase*, n.d., retrieved TK, <https://www.crunchbase.com/organization/sensetime#section-investors>.
37. Will Knight, "Paying with Your Face," *MIT Technology Review*, February 22, 2017, retrieved June 20, 2018, <https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/>; "Comet Labs," *Crunchbase*, n.d., retrieved TK, [https://www.crunchbase.com/search/funding\\_rounds/field/organizations/num\\_investments/comet-labs](https://www.crunchbase.com/search/funding_rounds/field/organizations/num_investments/comet-labs).
38. James Millward, "What It's Like to Live in a Surveillance State," *New York Times*, February 3, 2018, retrieved June 20, 2018, <https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uyghurs.html>.
39. Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times*, April 14, 2019, retrieved July 2, 2019, <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>.
40. Kurban Niyaz, "Authorities Require Uyghurs in Xinjiang's Aksu to Get Barcodes on Their Knives," *Radio Free Asia*, October 11, 2017, retrieved July 2, 2019, <https://www.rfa.org/english/news/uyghur/authorities-require-uyghurs-in-xinjiangs-aksu-to-get-barcodes-on-their-knives-10112017143950.html>.
41. Mallory Locklear, "Microsoft Calls on Congress to Regulate Facial Recognition," *Engadget*, July 13, 2018, retrieved August 5, 2018, <https://www.engadget.com/2018/07/13/microsoft-congress-regulate-facial-recognition/>.
42. "Study: Your Facebook Profile Picture Can Boost Your Chances of Being Interviewed by as Much as 40%," *Workopolis*, January 29, 2016, retrieved July 5, 2018, <https://careers.workopolis.com/advice/study-facebook-profile-picture-directly-affects-your-chances-of-being-interviewed-for-a-job/>.
43. "Data Brokers: A Call for Transparency and Accountability," *Federal Trade Commission*, May 2014, retrieved June 8, 2018, <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>, p. 8.
44. George Lowery, "Gut Instinct: We Can Identify Criminals on Sight, Study Finds," *Cornell Chronicle*, April 7, 2011, retrieved July 5, 2018, <http://news.cornell.edu/stories/2011/04/study-we-can-spot-criminals-photos>.
45. Dick Ahlstrom, "'Gut Instinct' Makes for Happy Relationship, Researchers Say," *Irish Times*, November 28, 2013, retrieved July 5, 2018, <https://www.irishtimes.com/news/science/gut-instinct-makes-for-happy-relationship-researchers-say-1.1610919>.
46. Sarah Young, "Gut Feelings Really Do Stop You from Making Mistakes, Study Finds," *Independent*, March 23, 2018, retrieved July 5, 2018, <https://www.independent.co.uk/life-style/gut-feelings-instinct-stop-mistakes-brain-signal-influence-emotions-study-findings-a8270611.html>.
47. Vivian Lam, "'We Know Very Little About the Brain': Experts Outline Challenges

- in Neuroscience,” *Scope* (Stanford Medicine blog), November 8, 2016, retrieved July 5, 2018, <https://scopeblog.stanford.edu/2016/11/08/challenges-in-neuroscience-in-the-21st-century/>.
48. “Google Search Statistics,” Internet Live Stats, n.d., retrieved August 12, 2018, <http://www.internetlivestats.com/google-search-statistics/#ref-7>.
  49. “How Search Works,” Google Search, n.d., retrieved August 12, 2018, [https://www.google.com/search/howsearchworks/responses/#?modal\\_active=none](https://www.google.com/search/howsearchworks/responses/#?modal_active=none).
  50. “Number of Mobile Phone Search Users in the United States from 2014 to 2020 (in Millions),” Statista, n.d., retrieved July 2, 2019, <https://www.statista.com/statistics/368746/us-mobile-search-users/>; “Distribution of Total and Mobile Organic Search Visits in the United States as of 1st Quarter 2019, by Engine,” Statista, April 24, 2019, retrieved July 2, 2019, <https://www.statista.com/statistics/625554/mobile-share-of-us-organic-search-engine-visits/>.
  51. J. R. Hebert et al., “Social Desirability Bias in Dietary Self-Report May Compromise the Validity of Dietary Intake Measures,” *International Journal of Epidemiology* 24, no. 2 (1995): 389–98.
  52. J. A. Karp and D. Brockington, “Social Desirability and Response Validity: A Comparative Analysis of Overreporting Voter Turnout in Five Countries,” *Journal of Politics* 67, no. 3 (2005): 825–40.
  53. C. G. Davis, J. Thake, and N. Vilhena, “Social Desirability Biases in Self-Reported Alcohol Consumption and Harms,” *Addictive Behaviors* 35, no. 4 (2010): 302–11.
  54. J. A. Catania et al., “Methodological Problems in AIDS Behavioral Research: Influences on Measurement Error and Participation Bias in Studies of Sexual Behavior,” *Psychological Bulletin* 108, no. 3 (1990): 339.
  55. Z. Lee and L. Woodliffe, “Donor Misreporting: Conceptualizing Social Desirability Bias in Giving Surveys,” *International Journal of Voluntary and Nonprofit Organizations* 21, no. 4 (2010): 569–87.
  56. Mark Murphy, “The Dunning-Kruger Effect Shows Why Some People Think They’re Great Even When Their Work Is Terrible,” *Forbes*, January 24, 2017, retrieved August 12, 2018, <https://www.forbes.com/sites/markmurphy/2017/01/24/the-dunning-kruger-effect-shows-why-some-people-think-theyre-great-even-when-their-work-is-terrible/#440e90e85d7c>.
  57. Sharon Epperson, “What It Takes to Become a Millionaire,” CNBC, September 19, 2011, retrieved August 12, 2018, <https://www.cnbc.com/id/44559645>.
  58. D. D. Johnson and J. H. Fowler, “The Evolution of Overconfidence,” *Nature* 477, no. 7364 (2011): 317–20.
  59. “The Evolution of Overconfidence,” *MIT Technology Review*, September 24, 2009, retrieved August 17, 2018, <https://www.technologyreview.com/s/415454/the-evolution-of-overconfidence/>.

## CHAPTER 6: THE ALL-KNOWING INTERNET OF THINGS

1. “The Internet of Things: The Future of Consumer Adoption,” Accenture, 2014, retrieved July 8, 2018, [www.accenture.com/t20150624T211456\\_w\\_/us-en/\\_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology\\_9/Accenture-Internet-Things.pdf](http://www.accenture.com/t20150624T211456_w_/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf).
2. D. S. Wie et al., “Wafer-Recyclable, Environment-Friendly Transfer Printing for Large-Scale Thin-Film Nanoelectronics,” *Proceedings of the National Academy of Sciences* 115 (2018): 201806640, retrieved August 5, 2018, <http://www.pnas.org/content/115/31/E7236>.
3. Purdue University, “Electronic Stickers to Streamline Large-Scale ‘Internet of Things,’” *Science Daily*, July 16, 2018, retrieved July 25, 2018, [www.sciencedaily.com/releases/2018/07/180716164508.htm](http://www.sciencedaily.com/releases/2018/07/180716164508.htm).
4. “Ericsson Mobility Report,” Ericsson, June 2016, retrieved July 8, 2018, [www.ericsson.com/mobility-report](http://www.ericsson.com/mobility-report).

- son.com/assets/local/mobility-report/documents/2016/Ericsson-mobility-report-june-2016.pdf.
5. Lee Rainie, "The Internet of Things Connectivity Binge: What Are the Implications?," Pew Research Center: Internet and Technology, June 6, 2017, retrieved July 8, 2018, [www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/](http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/).
  6. Kashmir Hill and Surya Mattu, "The House That Spied on Me," Gizmodo Media Group, February 7, 2018, retrieved July 8, 2018, <https://gizmodo.com/the-house-that-spied-on-me-1822429852>.
  7. Sapna Maheshwari, "How Smart TVs in Millions of U.S. Homes Track More Than What's on Tonight," *New York Times*, July 5, 2018, retrieved July 8, 2018, <https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html>.
  8. Kashmir Hill and Surya Mattu, "The House That Spied on Me," Gizmodo Media Group, February 7, 2018, retrieved July 8, 2018, <https://gizmodo.com/the-house-that-spied-on-me-1822429852>.
  9. 115th Congress (2017–2018), "S.J.Res.34: A Joint Resolution . . . Relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,'" Congress.gov, retrieved July 8, 2018, <https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34>.
  10. Andy Greenberg, "Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records," *WIRED*, June 27, 2018, retrieved July 8, 2018, <https://www.wired.com/story/exactis-database-leak-340-million-records/>.
  11. "Public Trust in Government: 1958–2017," Pew Research Center: US Politics and Policy, December 14, 2017, retrieved August 5, 2018, <http://www.people-press.org/2017/12/14/public-trust-in-government-1958–2017/>.
  12. This does not include a brief bump in public trust in government following the attacks of 9/11.
  13. Niall McCarthy, "The Institutions Americans Trust Most and Least in 2018," *Forbes*, June 29, 2018, retrieved August 5, 2018, <https://www.forbes.com/sites/niallmccarthy/2018/06/29/the-institutions-americans-trust-most-and-least-in-2018-in-fographic/#2475b3452fc8>.
  14. Home page, Sidewalk Labs, n.d., retrieved February 4, 2019, <https://www.sidewalklabs.com/>.
  15. Home page, Sidewalk Toronto, n.d., retrieved July 8, 2018, <https://sidewalktoronto.ca/>; Elizabeth Woyke, "A Smarter Smart City," *MIT Technology Review*, February 21, 2018, retrieved July 8, 2018, <https://www.technologyreview.com/s/610249/a-smarter-smart-city/>.
  16. "New District in Toronto Will Tackle the Challenges of Urban Growth," Sidewalk Toronto, October 17, 2017, retrieved July 8, 2018, <https://sidewalktoronto.ca/wp-content/uploads/2018/04/Sidewalk-Toronto-Press-Release.pdf>.
  17. "Project Vision," Sidewalk Labs, October 17, 2017, retrieved July 8, 2018, <https://sidewalktoronto.ca/wp-content/uploads/2017/10/Sidewalk-Labs-Vision-Sections-of-RFP-Submission.pdf>, p. 37.
  18. Nancy Scola, "Google Is Building a City of the Future in Toronto. Would Anyone Want to Live There?" *Politico*, July/August 2018, retrieved August 5, 2018, <https://www.politico.com/magazine/story/2018/06/29/google-city-technology-toronto-canada-218841>.
  19. Elon Musk, "Elon Musk First Principle Reasoning TED," YouTube, August 25, 2016, retrieved July 13, 2018, <https://www.youtube.com/watch?v=0JQXoSmC1rs>.
  20. Martine Powers, "The Real Reason Why Boston's Geography Is the Most Confusing Thing Ever," *Boston.com*, April 2, 2014, retrieved July 13, 2018, <https://www.boston.com/news/local-news/2014/04/02/the-real-reason-why-bostons-geography-is-the-most-confusing-thing-ever>.
  21. Charlie Sorrel, "How the iPhone Made Accessibility Accessible to Everyone," *Cult of Mac*, June 28, 2017, retrieved February 4, 2019, <https://www.cultofmac.com/488348/>

- iphone-accessibility/.
22. Vindu Goel, "At \$1,000, Apple's iPhone X Crosses a Pricing Threshold," *New York Times*, September 10, 2017, retrieved February 4, 2019, <https://www.nytimes.com/2017/09/10/technology/apple-iphone-price.html>.
  23. "Your New iPhone XS," Apple, n.d., retrieved February 4, 2019, [https://www.apple.com/shop/buy-iphone/iphone-xs/6.5-inch-display-512gb-gold-unlocked?afid=p238lsND54E8jO-dc\\_mtid\\_1870765e38482\\_pccrid\\_324289715177&cid=aos-us-kwgo-pla-iphone—slid—product-MT5J2LL/A](https://www.apple.com/shop/buy-iphone/iphone-xs/6.5-inch-display-512gb-gold-unlocked?afid=p238lsND54E8jO-dc_mtid_1870765e38482_pccrid_324289715177&cid=aos-us-kwgo-pla-iphone—slid—product-MT5J2LL/A).
  24. Justin Pritchard, "What Is the Average Monthly Mortgage Payment?," *Balance*, November 5, 2018, retrieved February 4, 2019, <https://www.thebalance.com/average-monthly-mortgage-payment-4154282>.
  25. "Map of Adaptive Traffic Control Systems in the US," Google Maps, n.d., retrieved July 8, 2018, [https://www.google.com/maps/d/u/0/viewer?ll=37.300274999999985%2C-99.40429699999999&spn=27.845221%2C57.041016&hl=en&t=h&gl=us&oe=UTF8&msa=0&z=5&source=embed&ie=UTF8&mid=17gN\\_VQSZfNA-olj7UB\\_QstT\\_z6E](https://www.google.com/maps/d/u/0/viewer?ll=37.300274999999985%2C-99.40429699999999&spn=27.845221%2C57.041016&hl=en&t=h&gl=us&oe=UTF8&msa=0&z=5&source=embed&ie=UTF8&mid=17gN_VQSZfNA-olj7UB_QstT_z6E).
  26. "Adaptive Traffic Control Systems: Domestic and Foreign State of Practice," National Academies of Science, Medicine, and Engineering, 2010, retrieved July 8, 2018, <https://www.nap.edu/download/14364>.
  27. Trevor Reed, "Global Traffic Scorecard," INRIX, February 2019, retrieved June 27, 2019, [file:///Users/alexiswichowski/Downloads/INRIX\\_2018\\_Global\\_Traffic\\_Scorecard\\_Report\\_final\\_.pdf](file:///Users/alexiswichowski/Downloads/INRIX_2018_Global_Traffic_Scorecard_Report_final_.pdf).
  28. Ashley Halsey, "There Are About 1.7 Million Rear-End Collisions on U.S. Roads Each Year. Here's How to Stop Them," *Washington Post*, June 8, 2015, retrieved July 8, 2018, [https://www.washingtonpost.com/news/dr-gridlock/wp/2015/06/08/there-are-about-1-7-million-rear-end-collisions-on-u-s-roads-each-year-heres-how-to-stop-them/?utm\\_term=.298fc176f77e](https://www.washingtonpost.com/news/dr-gridlock/wp/2015/06/08/there-are-about-1-7-million-rear-end-collisions-on-u-s-roads-each-year-heres-how-to-stop-them/?utm_term=.298fc176f77e).
  29. Michael Fleeman, "Google's Waze App Fires Back Against Police Criticism," *Verge*, March 29, 2015, retrieved July 13, 2018, [https://www.huffingtonpost.com/2015/01/27/waze-police-tracking-criticism\\_n\\_6558408.html](https://www.huffingtonpost.com/2015/01/27/waze-police-tracking-criticism_n_6558408.html).
  30. "Does Waze Put Police Officers' Lives at Risk?," *CBS News*, January 29, 2015, retrieved July 13, 2018, <https://www.cbsnews.com/news/does-waze-put-police-officers-lives-at-risk/>.
  31. "Mayor de Blasio and NYCEDC Launch Sixth Annual NYC Bigapps Competition: Challenging NYC's Tech Innovators to Find Lasting Solutions to Four of the City's Most Pressing Issues," *NYC Office of the Mayor*, July 17, 2015, retrieved July 13, 2018, <https://www1.nyc.gov/office-of-the-mayor/news/494-15/mayor-de-blasio-nycedc-launch-sixth-annual-nyc-bigapps-competition-challenging-nyc-s-tech>.
  32. "Critical Infrastructure Sectors," US Department of Homeland Security, n.d., retrieved February 4, 2019, <https://www.dhs.gov/cisa/critical-infrastructure-sectors>.
  33. Robert Atkinson et al., "A Policymaker's Guide to Digital Infrastructure," Information Technology and Innovation Foundation, May 2016, retrieved July 8, 2018, [http://www2.itif.org/2016-policymakers-guide-digital-infrastructure.pdf?\\_ga=2.125865421.1763289522.1531062137-2090438079.1531062137](http://www2.itif.org/2016-policymakers-guide-digital-infrastructure.pdf?_ga=2.125865421.1763289522.1531062137-2090438079.1531062137).
  34. Andrew Hawkins, "Elon Musk's Boring Company Approved to Build High-Speed Transit Between Downtown Chicago and O'Hare Airport," *Verge*, June 13, 2018, retrieved July 8, 2018, <https://www.theverge.com/2018/6/13/17462496/elon-musk-boring-company-approved-tunnel-chicago>.
  35. Elizabeth Shockman, "US Governments Have Made Some Big Flops in the World of Tech. Here's Why," *Science Friday*, November 9, 2015, retrieved July 8, 2018, <https://www.pri.org/stories/2015-11-09/us-governments-have-made-some-big-flops-world-tech-heres-why>.
  36. Niam Yaraghi, "Doomed: Challenges and Solutions to Government IT Projects," *Brookings Institution*, August 25, 2015, retrieved July 8, 2018, <https://www.brookings.edu/blog/techtank/2015/08/25/doomed-challenges-and-solutions-to-government-it-proj->

- ects/.
37. Venkat Motupalli, "How Big Data Is Changing Democracy," *Journal of International Affairs*, June 22, 2018, retrieved July 8, 2018, <https://jia.sipa.columbia.edu/how-big-data-changing-democracy#4>.
  38. Derek Powazek, "Nobody Uses Their Real Name Online, and Other Outdated Notions," Gizmodo Media Group, August 25, 2011, retrieved July 5, 2018, <https://gizmodo.com/5834112/nobody-uses-their-real-name-online-and-other-outdated-notions>.
  39. Brent Smith, "Two Decades of Recommender Systems at Amazon.com," IEEE Computer Society, May/June 2017, retrieved July 5, 2018, <https://www.computer.org/csdl/mags/ic/2017/03/mic2017030012.html>.
  40. "E-Stats," US Census Bureau, March 7, 2001, retrieved July 5, 2018, <https://www.census.gov/content/dam/Census/library/publications/2001/econ/1999estatstext.pdf>.
  41. Michael Martinez, "Amazon: Jeff Bezos' Juggernaut Began with a Recommender System That Launched a Thousand Algorithms," IEEE Computer Society, June 20, 2017, retrieved July 5, 2018, <https://publications.computer.org/internet-computing/2017/06/20/amazon-jeff-bezos-juggernaut-began-with-a-recommender-system-that-launched-a-thousand-algorithms/>.
  42. "And the Emmy Goes to . . . Amazon Instant Video!" Business Wire, August 2, 2013, retrieved July 5, 2018, <https://www.businesswire.com/news/home/20130802005131/en/Emmy-To%E2%80%A6Amazon-Instant-Video>.
  43. B. Lika, K. Kolomvatsos, and S. Hadjiefthymiades, "Facing the Cold Start Problem in Recommender Systems," *Expert Systems with Applications* 41, no. 4 (2014): 2065–73.
  44. Mehrdad Fatourehchi, "The Evolving Landscape of Recommendation Systems," TechCrunch, September 28, 2015, retrieved August 5, 2018, <https://techcrunch.com/2015/09/28/the-evolving-landscape-of-recommendation-systems/>.
  45. "Amazon's Privacy Notice," Amazon, n.d., retrieved July 5, 2018, <https://www.amazon.com/gp/help/customer/display.html?nodeId=468496>.
  46. "Percentage of Paid Units Sold by Third-Party Sellers on Amazon Platform as of 1st Quarter 2018," Statista, n.d., retrieved July 5, 2018, <https://www.statista.com/statistics/259782/third-party-seller-share-of-amazon-platform/>.
  47. Ranju Das, "Amazon Rekognition Announces Real-Time Face Recognition, Support for Recognition of Text in Image, and Improved Face Detection," *AWS Machine Learning* (blog), November 21, 2017, retrieved June 20, 2018, <https://aws.amazon.com/blogs/machine-learning/amazon-rekognition-announces-real-time-face-recognition-support-for-recognition-of-text-in-image-and-improved-face-detection/>.
  48. "Amazon Rekognition Customer Use Cases," Amazon Web Services, n.d., retrieved June 20, 2018, <https://aws.amazon.com/rekognition/customers/>.
  49. Chris Greenwood, "One CCTV Camera for Every 10 People: Report Says There Are Now Six Million Across the UK," *Daily Mail*, October 25, 2016, retrieved February 4, 2019, <https://www.dailymail.co.uk/news/article-3872818/One-CCTV-camera-10-people-Report-says-six-million-UK-useless.html>.
  50. Jon Russell, "China's CCTV Surveillance Network Took Just 7 Minutes to Capture BBC Reporter," TechCrunch, February 4, 2018, retrieved February 4, 2019, <https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/>.
  51. "Amazon Rekognition FAQs: Data Privacy," Amazon Web Services, n.d., retrieved February 5, 2019, <https://aws.amazon.com/rekognition/faqs/>.
  52. American Civil Liberties Union, records request to the Orlando Police Department, January 18, 2018, retrieved July 2, 2019, [https://www.aclunc.org/docs/20180522\\_ARD.pdf#page=53](https://www.aclunc.org/docs/20180522_ARD.pdf#page=53).
  53. Nick Wingfield, "Amazon Pushes Facial Recognition to Police. Critics See Surveillance Risk," *New York Times*, May 22, 2018, retrieved June 20, 2018, <https://www.nytimes.com/2018/05/22/technology/amazon-facial-recognition.html>.

54. Brian Heater, "Congress Members Demand Answers from Amazon About Facial Recognition Software," *TechCrunch*, July 26, 2018, retrieved February 5, 2019, <https://techcrunch.com/2018/07/26/congress-members-demand-answers-from-amazon-about-facial-recognition-software/>.
55. Larry Hardesty, "Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems," *MIT News*, February 11, 2018, retrieved June 20, 2018, <http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>; Molly Wood, "Why Facial Recognition Software Has Trouble Recognizing People of Color," *Marketplace*, February 13, 2018, retrieved June 27, 2019, <https://www.marketplace.org/2018/02/13/why-algorithms-may-have-trouble-recognizing-your-face/>.
56. Derek Hawkins, "Lawmakers Worry Amazon's Facial Recognition Tech Could Reinforce Racial Profiling," *Washington Post*, May 29, 2018, retrieved February 5, 2019, [https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/29/the-cybersecurity-202-lawmakers-worry-amazon-s-facial-recognition-tech-could-reinforce-racial-profiling/5b0c10741b326b492dd07eb8/?utm\\_term=.1f866dbed0a5](https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/29/the-cybersecurity-202-lawmakers-worry-amazon-s-facial-recognition-tech-could-reinforce-racial-profiling/5b0c10741b326b492dd07eb8/?utm_term=.1f866dbed0a5).
57. Evgeny Morozov, "Will Tech Giants Move on from the Internet, Now We've All Been Harvested?" *Guardian*, January 27, 2018, retrieved July 14, 2018, <https://www.theguardian.com/technology/2018/jan/28/morozov-artificial-intelligence-data-technology-online>.
58. "The Fate of Online Trust in the Next Decade," Pew Research Center: Internet and Technology, August 10, 2017, retrieved July 14, 2018, <http://www.pewinternet.org/2017/08/10/theme-3-trust-will-not-grow-but-technology-usage-will-continue-to-rise-as-a-new-normal-sets-in/>.

## CHAPTER 7: THE MIND, IMMERSED

1. D. Glassbrenner, "Estimating the Lives Saved by Safety Belts and Air Bags," *Age 5* (2016): 12; "Air Bags," National Highway Traffic Safety Administration, US Department of Transportation, n.d., retrieved April 21, 2019, <https://www.nhtsa.gov/equipment/air-bags>.
2. "National Household Travel Survey Daily Travel Quick Facts," *Bureau of Transportation Statistics*, n.d., retrieved August 5, 2018, [www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/subject\\_areas/national\\_household\\_travel\\_survey/daily\\_travel.html](http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/subject_areas/national_household_travel_survey/daily_travel.html).
3. B. R. Burdett et al., "Not All Minds Wander Equally: The Influence of Traits, States and Road Environment Factors on Self-Reported Mind Wandering During Everyday Driving," *US National Library of Medicine, National Institutes of Health*, October 2016, retrieved August 5, 2018, [www.ncbi.nlm.nih.gov/pubmed/27372440](http://www.ncbi.nlm.nih.gov/pubmed/27372440).
4. "Distracted Driving 2015," National Highway Traffic Safety Administration, US Department of Transportation, March 2017, retrieved August 5, 2018, [https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812\\_381\\_distracteddriving2015.pdf](https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812_381_distracteddriving2015.pdf).
5. Ioannis Pavlidis, "Dissecting Driver Behaviors Under Cognitive, Emotional, Sensorimotor, and Mixed Stressors," *Nature*, May 12, 2016, retrieved August 5, 2018, [www.nature.com/articles/srep25651.pdf](http://www.nature.com/articles/srep25651.pdf).
6. University of Houston, "'Sixth Sense' Protects Drivers Except When Texting," *Science Daily*, May 12, 2016, retrieved August 5, 2018, [www.sciencedaily.com/releases/2016/05/160512084547.htm](http://www.sciencedaily.com/releases/2016/05/160512084547.htm).
7. J. L. Nasar and D. Troyer, "Pedestrian Injuries Due to Mobile Phone Use in Public Places," *Accident Analysis and Prevention* 57 (2013): 91–95, <https://doi.org/10.1016/j.aap.2013.03.021>.
8. "Head Up, Phone Down When Headed Back to School," National Safety Council, n.d., retrieved April 21, 2019, <https://www.nsc.org/home-safety/safety-topics/distracted-walking/teens>.
9. "Apple iMac G3/333 (Fruit Colors) Specs," *EveryMac*, n.d., retrieved July 13, 2018,

- [https://everymac.com/systems/apple/imac/specs/imac\\_333.html](https://everymac.com/systems/apple/imac/specs/imac_333.html).
10. "iMac (Rev. C)," Apple History, n.d., retrieved August 5, 2018, <https://apple-history.com/imacrevc>.
  11. Lea Winerman, "Smarter Than Ever?," *American Psychological Association Monitor* 44, no. 3 (March 2013): 30, retrieved July 14, 2018, <http://www.apa.org/monitor/2013/03/smarter.aspx>.
  12. Kenneth Simon, *Digest of Educational Statistics*, Office of Education Bulletin, no. 4 (Washington, DC: US Government Printing Office, 1965).
  13. "Educational Attainment in the United States: 2015," US Census Bureau, n.d., retrieved July 13, 2018, <https://www.census.gov/content/dam/Census/library/publications/2016/demo/p20-578.pdf>.
  14. "Percentage of Americans with College Degrees Rises, Paying for Degrees Tops Financial Challenges," PBS NewsHour, April 22, 2014, retrieved July 13, 2018, <https://www.pbs.org/newshour/education/percentage-americans-college-degrees-rises-paying-degrees-tops-financial-challenges>; J. Shaw, "Statistics of College Graduates," *Quarterly Publications of the American Statistical Association* 17, no. 131 (1920): 335–41, retrieved July 13, 2018, <http://www.jstor.org/stable/2965351>.
  15. M. Tommasi et al., "Increased Educational Level Is Related with Higher IQ Scores but Lower G-Variance: Evidence from the Standardization of the WAIS-R for Italy," *Intelligence* 50 (2015): 68–74; Stuart J. Ritchie and Elliot M. Tucker-Drob, "How Much Does Education Improve Intelligence? A Meta-Analysis," *Psychological Science* 29, no. 8 (2018): 1358–69.
  16. John Horrigan, "Lifelong Learning and Technology," Pew Research Center: Internet and Technology, March 22, 2016, retrieved August 5, 2018, <http://www.pewinternet.org/2016/03/22/lifelong-learning-and-technology/>.
  17. Kristen Purcell, "Americans Feel Better Informed Thanks to the Internet," Pew Research Center: Internet and Technology, December 8, 2014, retrieved August 5, 2018, <http://www.pewinternet.org/2014/12/08/better-informed/>.
  18. Lea Winerman, "Smarter Than Ever?," *American Psychological Association Monitor* 44, no. 3 (March 2013): 30, retrieved July 14, 2018, <http://www.apa.org/monitor/2013/03/smarter.aspx>.
  19. Karen Turner, "Lots of Coders Are Self-Taught, According to Developer Survey," *Washington Post*, March 30, 2016, retrieved July 13, 2018, [https://www.washingtonpost.com/news/the-switch/wp/2016/03/30/lots-of-coders-are-self-taught-according-to-developer-survey/?utm\\_term=.9e26cc363750](https://www.washingtonpost.com/news/the-switch/wp/2016/03/30/lots-of-coders-are-self-taught-according-to-developer-survey/?utm_term=.9e26cc363750).
  20. Kristen Purcell, "Search and Email Still Top the List of Most Popular Online Activities," *Pew Research Center: Internet and Technology*, August 9, 2011, retrieved July 15, 2018, <http://www.pewinternet.org/2011/08/09/search-and-email-still-top-the-list-of-most-popular-online-activities/>; "Number of Explicit Core Search Queries Powered by Search Engines in the United States as of January 2019 (in Billions)," Statista, n.d., retrieved June 27, 2019, <https://www.statista.com/statistics/265796/us-search-engines-ranked-by-number-of-core-searches/>.
  21. "Year in Search: 2017," Google Trends, n.d., retrieved July 13, 2018, <https://trends.google.com/trends/yis/2017/US/>.
  22. Doug Criss, "The Las Vegas Attack Is the Deadliest Mass Shooting in Modern US History," CNN, October 2, 2017, retrieved July 13, 2018, <https://www.cnn.com/2017/10/02/us/las-vegas-attack-deadliest-us-mass-shooting-trnd/index.html>.
  23. Nick Statt, "Google Will Stop Showing Search Results as You Type Because It Makes No Sense on Mobile," *Verge*, July 26, 2017, retrieved July 13, 2018, <https://www.theverge.com/2017/7/26/16034844/google-kills-off-instant-search-for-mobile-consistency>.
  24. Tomas Chamorro-Premuzic, "Curiosity Is as Important as Intelligence," *Harvard Business Review*, August 27, 2014, retrieved July 13, 2018, <https://hbr.org/2014/08/curiosity-is-as-important-as-intelligence>.
  25. J. Holmes, *Nonsense: The Power of Not Knowing* (New York: Broadway Books, 2016).

26. P. Merrotsy, "Tolerance of Ambiguity: A Trait of the Creative Personality?," *Creativity Research Journal* 25, no. 2 (2013): 232–37.
27. Amy Thompson, "How Learning a New Language Improves Tolerance," Conversation, December 11, 2016, retrieved July 13, 2018, <https://theconversation.com/how-learning-a-new-language-improves-tolerance-68472>; S. M. Andersen and A. H. Schwartz, "Intolerance of Ambiguity and Depression: A Cognitive Vulnerability Factor Linked to Hopelessness," *Social Cognition* 10, no. 3 (1992): 271–98.
28. "Americans Check Their Phones 80 Times a Day: Study," NBC News, November 11, 2017, retrieved July 14, 2018, <https://www.nbcnews.com/nightly-news/video/americans-check-their-smartphones-80-times-a-day-study-1093857859881>.
29. "Internet/Broadband Fact Sheet," Pew Research Center: Internet and Technology, February 5, 2018, retrieved June 20, 2018, <http://www.pewinternet.org/fact-sheet/internet-broadband/>.
30. Monica Anderson, "10% of Americans Don't Use the Internet. Who Are They?" Pew Research Center: Fact Tank, April 22, 2019, retrieved July 2, 2019, <https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/>.
31. Nick Bilton, "Steve Jobs Was a Low-Tech Parent," *New York Times*, September 10, 2014, retrieved June 20, 2018, <https://www.nytimes.com/2014/09/11/fashion/steve-jobs-apple-was-a-low-tech-parent.html>.
32. Leanna Garfield, "These Tech Execs Have Regrets About the World-Changing Sites They Helped Create," Business Insider, December 23, 2017, retrieved June 20, 2018, <http://www.businessinsider.com/social-media-affects-society-tech-execs-2017-12#former-facebook-president-sean-parker-has-said-the-network-changes-your-relationship-with-society-2>.
33. Steve Kovach, "Former Facebook Exec Feels 'Tremendous Guilt' for What He Helped Make," Business Insider, December 11, 2017, retrieved June 20, 2018, <http://www.businessinsider.com/former-facebook-exec-chamath-palihapitiya-social-media-damaging-society-2017-12>.
34. David Ginsberg, "Hard Questions: Is Spending Time on Social Media Bad for Us?" Facebook Newsroom, December 14, 2017, <https://newsroom.fb.com/news/2017/12/hard-questions-is-spending-time-on-social-media-bad-for-us/>.
35. "Why a Dodgy Social Media Profile Is Better Than None," Undercover Recruiter, retrieved June 20, 2018, <https://theundercoverrecruiter.com/why-no-social-media-presence-is-bigger-red-flag/>.
36. M. Pielot et al., "An In-Situ Study of Mobile Phone Notifications," *Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services* (September 2014): 233–242.
37. S. K. Kim et al., "An Analysis of the Effects of Smartphone Push Notifications on Task Performance with Regard to Smartphone Overuse Using ERP," *Computational Intelligence and Neuroscience* 3 (2016): 1–8.
38. M. Drouin, D. H. Kaiser, and D. A. Miller, "Phantom Vibrations Among Undergraduates: Prevalence and Associated Psychological Characteristics," *Computers in Human Behavior* 28, no. 4 (2012): 1490–96.
39. "Ledger of Harms," Center for Humane Technology, December 14, 2018, retrieved February 5, 2019, <https://ledger.humanetech.com/>.
40. "Americans Check Their Phones 80 Times a Day: Study," NBC News, November 11, 2017, retrieved July 14, 2018, <https://www.nbcnews.com/nightly-news/video/americans-check-their-smartphones-80-times-a-day-study-1093857859881>.
41. "Screw Emotional Intelligence: Here's the Key to the Future of Work," *Fast Company*, January 29, 2018, retrieved July 15, 2018, <https://www.fastcompany.com/40522394/screw-emotional-intelligence-heres-the-real-key-to-the-future-of-work>.
42. "These Are the Long-Term Effects of Multitasking," *Fast Company*, March 1, 2016, re-

- trieved July 13, 2018, <https://www.fastcompany.com/3057192/these-are-the-long-term-effects-of-multitasking>.
43. S. Leroy, "Why Is It So Hard to Do My Work? The Challenge of Attention Residue When Switching Between Work Tasks," *Organizational Behavior and Human Decision Processes* 109, no. 2 (2009): 168–81.
  44. "These Are the Long-Term Effects of Multitasking," *Fast Company*, March 1, 2016, retrieved July 13, 2018, <https://www.fastcompany.com/3057192/these-are-the-long-term-effects-of-multitasking>.
  45. Verne Kopytoff, "Where Pagers Haven't Gone Extinct Yet," *Fortune*, July 16, 2013, retrieved July 15, 2018, <http://fortune.com/2013/07/16/where-pagers-havent-gone-extinct-yet/>.
  46. R. Kegan and L. L. Lahey, *Immunity to Change: How to Overcome It and Unlock Potential in Yourself and Your Organization* (Brighton, MA: Harvard Business Review Press, 2009).
  47. J. Mittell, "Narrative Complexity in Contemporary American Television," *Velvet Light Trap* 58, no. 1 (2006): 29–40.
  48. A. J. Westphal et al., "Episodic Memory Retrieval Benefits from a Less Modular Brain Network Organization," *Journal of Neuroscience* (2017): 2509–16, retrieved July 13, 2018, <https://www.ncbi.nlm.nih.gov/pubmed/28242796>.
  49. Paul Zak, "Why Your Brain Loves Good Storytelling," *Harvard Business Review*, October 28, 2014, retrieved July 13, 2018, <https://hbr.org/2014/10/why-your-brain-loves-good-storytelling>.
  50. Annie Murphy Paul, "Your Brain on Fiction," *New York Times*, March 17, 2012, retrieved July 13, 2018, <https://www.nytimes.com/2012/03/18/opinion/sunday/the-neuroscience-of-your-brain-on-fiction.html?pagewanted=all>.
  51. B. Deen and G. McCarthy, "Reading About the Actions of Others: Biological Motion Imagery and Action Congruency Influence Brain Activity," *Neuropsychologia* 48, no. 6 (2010): 1607–15.
  52. Caroline Cakebread, "Millennials Are Making Advertisers' Lives Harder by Watching Less TV Than Their Predecessors," *Business Insider*, August 25, 2017, retrieved July 13, 2018, <http://www.businessinsider.com/millennials-watching-less-tv-than-previous-generations-chart-2017-8>.
  53. "Reading on the Rise: A New Chapter in American Literacy," National Endowment for the Arts, 2009, retrieved July 15, 2018, <https://www.arts.gov/sites/default/files/ReadingonRise.pdf>.
  54. Andrew Perrin, "Who Doesn't Read Books in America?" Pew Research Center: Internet and Technology, March 23, 2018, retrieved July 15, 2018, <http://www.pewinternet.org/2016/09/01/book-reading-2016/>.
  55. I first explored this idea in a coauthored piece with John S. Johnson: "Immerse Me: How to Get Lost in Story (Story Not Required)," *TechCrunch*, November 26, 2015, retrieved July 15, 2018, <https://techcrunch.com/2015/11/26/immerse-me-how-to-get-lost-in-story-actual-story-not-required/>.
  56. Oscar Raymundo, "Tim Cook: Augmented Reality Will Be an Essential Part of Your Daily Life, Like the iPhone," *Macworld*, October 3, 2016, retrieved June 27, 2019, <https://www.macworld.com/article/3126607/tim-cook-augmented-reality-will-be-an-essential-part-of-your-daily-life-like-the-iphone.html>.
  57. "16 Cool Things You Can Do with Google Glass," *PC Magazine*, April 15, 2014, retrieved July 15, 2018, <https://www.pcmag.com/feature/308711/16-cool-things-you-can-do-with-google-glass/15>.
  58. Victoria Turk, "One Year On, Who Still Plays Pokémon Go?," *WIRED*, July 6, 2017, retrieved July 15, 2018, <http://www.wired.co.uk/article/pokemon-go-first-anniversary-who-still-plays>.
  59. "Why Pokémon Go Has Been a Viral Success," *Business Insider*, July 13, 2016, retrieved July 15, 2018, <http://www.businessinsider.com/why-pokemon-go-has-been-a-viral>

- success-2016-7.
60. "Apple: Augmented Reality," Apple, n.d., retrieved July 15, 2018, <https://www.apple.com/ios/augmented-reality/>.
  61. Lee Raine et al., "The Rise of E-Reading," Pew Research Center: Internet and Technology, April 4, 2012, retrieved July 15, 2018, <http://libraries.pewinternet.org/2012/04/04/the-rise-of-e-reading/>.
  62. Larry Magid, "How (and Why) to Turn Off Google's Personalized Search Results," *Forbes*, January 13, 2012, retrieved July 15, 2018, <https://www.forbes.com/sites/larrymagid/2012/01/13/how-and-why-to-turn-off-googles-personalized-search-results/#2e4b284a38f2>.
  63. Lucas Matney, "Apple Delivers Big Updates to Its Augmented Reality Platform," TechCrunch, June 4, 2018, retrieved July 15, 2018, <https://techcrunch.com/2018/06/04/apple-delivers-big-updates-to-its-augmented-reality-platform/>.
  64. Art Lindsley, "C. S. Lewis on Absolutes," *Knowing & Doing*, Fall 2002, retrieved June 27, 2019, [http://www.cslewisinstitute.org/CS\\_Lewis\\_on\\_Absolutes](http://www.cslewisinstitute.org/CS_Lewis_on_Absolutes), p. 6.
  65. Michelle Fitzsimmons, "Apple's Tim Cook: 'AR Has the Ability to Amplify Human Performance,'" TechRadar, February 2, 2018, retrieved July 15, 2018, <https://www.techradar.com/news/apples-tim-cook-ar-has-the-ability-to-amplify-human-performance>.
  66. J. A. Bonus, A. Peebles, M. L. Mares, and I. G. Sarmiento, "Look on the Bright Side (of Media Effects): Pokémon Go as a Catalyst for Positive Life Experiences," *Media Psychology* 21, no. 2 (2018): 263–87.
  67. Stefan Hall, "Augmented and Virtual Reality: The Promise and Peril of Immersive Technologies," McKinsey, October 2017, retrieved August 8, 2018, <https://www.mckinsey.com/industries/media-and-entertainment/our-insights/augmented-and-virtual-reality-the-promise-and-peril-of-immersive-technologies>.
  68. David Phelan, "Apple CEO Tim Cook: As Brexit Hangs over UK, 'Times Are Not Really Awful, There's Some Great Things Happening,'" *Independent*, February 10, 2017, retrieved August 8, 2018, <https://www.independent.co.uk/life-style/gadgets-and-tech/features/apple-tim-cook-boss-brexit-uk-theresa-may-number-10-interview-ustwo-a7574086.html>.
  69. Shara Tibken, "Apple's Working on a Powerful, Wireless Headset for Both AR, VR," *CNET*, April 27, 2018, retrieved August 8, 2018, <https://www.cnet.com/news/apple-is-working-on-an-ar-augmented-reality-vr-virtual-reality-headset-powered-by-a-wireless-wigig-hub/?ftag=COS-05-10aaa0b&linkId=51043835>.

## CHAPTER 8: A DECLARATION OF CITIZEN-USER RIGHTS

1. J. E. Cohen, "The Historical Memory of American Presidents in the Mass Public," *Social Sciences* 7, no. 3 (2018): 36.
2. Rob Neufeld, "Portrait of the Past: Theodore Roosevelt in Asheville," *Citizen Times*, September 25, 2014, retrieved August 17, 2018, <https://www.citizen-times.com/story/life/2014/09/25/portrait-past-theodore-roosevelt-asheville/16239399/>.
3. R. C. V. Meyers, *Theodore Roosevelt, Patriot and Statesman: The True Story of an Ideal American* (Philadelphia: Ziegler, 1902).
4. "Trust in Judicial Branch Up, Executive Branch Down," Gallup, September 20, 2017, retrieved August 12, 2018, <https://news.gallup.com/poll/219674/trust-judicial-branch-executive-branch-down.aspx>; "Confidence in Institutions," Gallup, n.d., retrieved August 12, 2018, <https://news.gallup.com/poll/1597/confidence-institutions.aspx>.
5. "73% Say Freedom of Speech Worth Dying For," *Rasmussen Reports*, August 23, 2017, retrieved August 12, 2018, [http://www.rasmussenreports.com/public\\_content/life-style/general\\_lifestyle/august\\_2017/73\\_say\\_freedom\\_of\\_speech\\_worth\\_dying\\_for](http://www.rasmussenreports.com/public_content/life-style/general_lifestyle/august_2017/73_say_freedom_of_speech_worth_dying_for).
6. "Freedom Rings in Places You Might Not Expect," Gallup, June 27, 2018, retrieved August 12, 2018, [https://news.gallup.com/opinion/gallup/235973/freedom-rings-places-not-expect.aspx?g\\_source=link\\_news9&g\\_campaign=item\\_236411&g\\_medium=copy](https://news.gallup.com/opinion/gallup/235973/freedom-rings-places-not-expect.aspx?g_source=link_news9&g_campaign=item_236411&g_medium=copy).

7. "Mass Shootings," Gun Violence Archive, n.d., retrieved August 20, 2018, <https://www.gunviolencearchive.org/reports/mass-shooting?year=2015>; "mass shooting" is defined as more than four people killed in an incident, not including the shooter and not including those injured, "General Methodology," Gun Violence Archive, n.d., retrieved August 20, 2018, <http://www.gunviolencearchive.org/methodology>.
8. "Drug Overdose Death Data," Centers for Disease Control and Prevention, n.d., retrieved August 20, 2018, <https://www.cdc.gov/drugoverdose/data/statedeaths.html>.
9. "Opioid Overdose Crisis," National Institute on Drug Abuse, January 2019, retrieved July 2, 2019, <https://www.drugabuse.gov/drugs-abuse/opioids/opioid-overdose-crisis#one>.
10. "Deaths: Final Data for 2015," *National Vital Statistics Reports* (a publication of the Centers for Disease Control and Prevention) 66, no. 6 (November 27, 2017), retrieved August 20, 2018, [https://www.cdc.gov/nchs/data/nvsr/nvsr66/nvsr66\\_06.pdf](https://www.cdc.gov/nchs/data/nvsr/nvsr66/nvsr66_06.pdf).
11. "Deaths: Final Data for 2015," *National Vital Statistics Reports* (a publication of the Centers for Disease Control and Prevention) 66, no. 6 (November 27, 2017), retrieved August 20, 2018, [https://www.cdc.gov/nchs/data/nvsr/nvsr66/nvsr66\\_06.pdf](https://www.cdc.gov/nchs/data/nvsr/nvsr66/nvsr66_06.pdf).
12. It should be noted that prior to the 1950s, youth suicides were generally categorized by medical professionals as "accidents" and rarely discussed outside academic circles. The earliest reporting on the topic in academia emerged in the 1940s, for instance: K. Friedlander, "On the 'Longing to Die,'" *International Journal of Psychoanalysis* 21, (1940): 416; Jason Hanna, "Suicides Under Age 13: One Every 5 Days," *CNN*, August 14, 2017, retrieved August 20, 2018, <https://www.cnn.com/2017/08/14/health/child-suicides/index.html>.
13. "A Global Report on the Decline of Democracy," Council on Foreign Relations, April 17, 2018, retrieved August 20, 2018, <https://www.cfr.org/news-releases/global-report-decline-democracy>.
14. "Attacks on the Record: The State of Global Press Freedom, 2017–2018," Freedom House, n.d., retrieved August 20, 2018, <https://freedomhouse.org/report/special-reports/attacks-record-state-global-press-freedom-2017-2018>.
15. "Overview Fact Sheet," Freedom House, 2017, retrieved August 20, 2018, <https://freedomhouse.org/report/overview-fact-sheet>.
16. Niraj Chokshi, "It's Not Just You: 2017 Was Rough for Humanity, Study Finds," *New York Times*, September 12, 2018, retrieved September 16, 2018, <https://www.nytimes.com/2018/09/12/world/humanity-stress-sadness-pain.html?rref=collection%2Fsectioncollection%2Fscience&login=smartlock&auth=login-smartlock>.
17. "'Depression: Let's Talk' Says WHO, as Depression Tops List of Causes of Ill Health," World Health Organization, June 30, 2017, retrieved August 20, 2018, <http://www.who.int/mediacentre/news/releases/2017/world-health-day/en/>.
18. Megan A. Moreno et al., "Feeling Bad on Facebook: Depression Disclosures by College Students on a Social Networking Site," *Depression and Anxiety* 28, no. 6 (2011): 447–455.
19. "Ransomware Prevention and Response for CISOs," Federal Bureau of Investigation, n.d., retrieved August 20, 2018, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.
20. Natasha Lomas and Romain Dillet, "Terms of Service: The Biggest Lie of Our Industry," *TechCrunch*, August 21, 2015, retrieved August 19, 2018, <https://techcrunch.com/2015/08/21/agree-to-disagree/>.
21. "Apple Media Services Terms and Conditions," Apple, n.d., retrieved August 19, 2018, <https://www.apple.com/legal/internet-services/itunes/us/terms.html>.
22. "Google Terms of Service," Google, n.d., retrieved August 19, 2018, <https://policies.google.com/terms>.
23. "Terms of Service," Facebook, n.d., retrieved August 19, 2018, <https://www.facebook.com/terms.php>.
24. "Conditions of Use," Amazon, n.d., retrieved August 17, 2018, <https://www.amazon>.

- com/gp/help/customer/display.html?nodeId=508088.
25. "Terms of Service," Microsoft, n.d., retrieved August 19, 2018, <https://www.microsoft.com/en-us/servicesagreement/>.
  26. A. M. McDonald and L. F. Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* 4 (2008): 543; Alexis Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days," *Atlantic*, March 1, 2012, retrieved August 19, 2018, <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>.
  27. "The Rumors Are True: We Spend More and More Time Online," TechCrunch, December 23, 2009, retrieved August 19, 2018, <https://techcrunch.com/2009/12/23/harris-interactive-poll/>.
  28. Jacqueline Howard, "Americans Devote More Than 10 Hours a Day to Screen Time, and Growing," *CNN*, July 29, 2016, retrieved August 19, 2018, <https://www.cnn.com/2016/06/30/health/americans-screen-time-nielsen/index.html>.
  29. "How Long Do Users Stay on Web Pages?," Nielsen & Norman Group, September 12, 2011, retrieved August 19, 2018, <https://www.nngroup.com/articles/how-long-do-users-stay-on-web-pages/>.
  30. Malcolm Owen, "Apple, Other Tech Companies Continue to Resist Encryption Backdoor Proposals by FBI, U.S. DOJ," *AppleInsider*, May 2, 2018, retrieved August 20, 2018, <https://appleinsider.com/articles/18/05/02/apple-other-tech-companies-continue-to-resist-encryption-backdoor-proposals-by-fbi-us-doj>.
  31. Kirsten Korosec, "The 25 Most Common Passwords of 2017 Include 'Star Wars,'" *Fortune*, December 19, 2017, retrieved August 20, 2018, <http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/>.
  32. "Terms of Service," Facebook, n.d., retrieved August 19, 2018, <https://www.facebook.com/terms.php>.
  33. "Conditions of Use," Amazon, n.d., retrieved August 17, 2018, <https://www.amazon.com/gp/help/customer/display.html?nodeId=508088>.
  34. Lee Raine, "The State of Privacy in Post-Snowden America," Pew Research Center: Fact Tank, September 21, 2016, retrieved August 20, 2018, <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>.
  35. Caroline Cakebread, "You're Not Alone, No One Reads Terms of Service Agreements," *Business Insider*, November 11, 2017, retrieved August 20, 2018, <https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11>.
  36. S. Kokolakis, "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers and Security* 64 (2017): 122–34.
  37. C. Hallam and G. Zanella, "Online Self-Disclosure: The Privacy Paradox Explained as a Temporally Discounted Balance Between Concerns and Rewards," *Computers in Human Behavior* 68 (2017): 217–27.
  38. Aaron Smith, "Record Shares of Americans Now Own Smartphones, Have Home Broadband," Pew Research Center: Fact Tank, January 12, 2017, retrieved August 20, 2018, <http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/>.
  39. Gloria Guzman, "Household Income: 2016," US Census Bureau, September 2017, retrieved August 20, 2018, <https://www.census.gov/content/dam/Census/library/publications/2017/acs/acsbr16-02.pdf>.
  40. Selena Maranjian, "'What Tax Bracket Am I In?'—'It's Complicated,'" *Motley Fool*, April 26, 2013, retrieved August 20, 2018, <https://www.fool.com/investing/general/2013/04/26/what-tax-bracket-am-i-in-its-complicated.aspx>.
  41. Bree Fowler, "Best Low-Cost Cell-Phone Plans," *Consumer Reports*, August 12, 2018, retrieved August 20, 2018, <https://www.consumerreports.org/cell-phone-plans/best-low-cost-cell-phone-plans/>; Eli Blumenthal, "Internet Bill Too High? Here's How to

- Save," *USA Today*, January 8, 2018, retrieved August 20, 2018, <https://www.usatoday.com/story/money/personalfinance/budget-and-spending/2018/01/08/internet-bill-too-high-heres-how-save/429890001/>.
42. "Apple Music Plans," Apple, n.d., retrieved August 20, 2018, <https://www.apple.com/apple-music/plans/>; "Google One," Google, n.d., retrieved August 20, 2018, <https://one.google.com/getupdates>.
  43. "Right to Be Forgotten," General Data Protection Regulation (GDPR), n.d., retrieved August 20, 2018, <https://gdpr-info.eu/issues/right-to-be-forgotten/>.
  44. Lucas Laursen, "How Google Handled a Year of 'Right to Be Forgotten' Requests," *IEEE Computer Society*, April 23, 2015, retrieved August 20, 2018, <https://spectrum.ieee.org/telecom/internet/how-google-handled-a-year-of-right-to-be-forgotten-requests>.
  45. "The Size of the World Wide Web (the Internet)," World Wide Web Size, n.d., retrieved August 20, 2018, <http://www.worldwidewebsize.com/>.
  46. "Verisign Domain Name Industry Brief; Internet Grows to 330.6 Million Domain Names in Q1 2017," Verisign, July 18, 2017, retrieved August 20, 2018, <https://blog.verisign.com/domain-names/verisign-domain-name-industry-brief-internet-grows-to-330-6-million-domain-names-in-q1-2017/>.
  47. Rachel Kraus, "Europeans Asked Google for Their 'Right to Be Forgotten' 2.4 million times," Mashable, February 28, 2018, retrieved August 20, 2018, <https://mashable.com/2018/02/27/right-to-be-forgotten-google-transparency-report/#r1C3LUVYSQn>.
  48. "Freedom of Information Act," FOIA, n.d., retrieved August 22, 2018, <https://www.foia.gov/faq.html>.
  49. "Right of Access," General Data Protection Regulation, EU, n.d., retrieved August 22, 2018, <https://www.gdpreu.org/the-regulation/list-of-data-rights/right-of-access/>.
  50. Olivia Solon, "New Europe Law Makes It Easy to Find Out What Your Boss Has Said About You," *Guardian*, April 24, 2018, retrieved August 23, 2018, <https://www.theguardian.com/technology/2018/apr/23/europe-gdpr-data-law-employer-employee>.
  51. "Article 83: General Conditions for Imposing Administrative Fines," General Data Protection Regulation, EU, retrieved August 23, 2018, <https://gdpr-info.eu/art-83-gdpr/>.
  52. "Our Membership," British Medical Association, n.d., retrieved August 23, 2018, <https://www.bma.org.uk/membership>.
  53. Valeria Fiore, "GPs Asked to Lobby MPs over 'Bombardment' of Patient Data Requests," *Pulse Today*, August 10, 2018, retrieved August 23, 2018, <http://www.pulsetoday.co.uk/news/gp-topics/it/gps-asked-to-lobby-mps-over-bombardment-of-patient-data-requests/20037259.article>.
  54. Andrew Ross, "82% of Organisations Do Not Know Where All Their Critical Data Is Kept, Says Research," *Information Age*, August 21, 2018, retrieved August 23, 2018, <https://www.information-age.com/critical-data-123474315/>.
  55. A. G. Tansley, "The Use and Abuse of Vegetational Concepts and Terms," *Ecology* 16, no. 3 (1935): 284–307.
  56. F. Stuart Chapin, Pamela A. Matson, and Harold A. Mooney, *Principles of Terrestrial Ecosystem Ecology* (New York: Springer, 2002), 281–304.
  57. Tim Herrera, "When You Track Oreos, Exercise and Everything Else," *New York Times*, August 15, 2018, retrieved August 17, 2018, <https://www.nytimes.com/2018/08/15/technology/personaltech/track-your-life-app.html>.
  58. "UN Refugee Agency: Record 65.6 Million People Displaced Worldwide," *BBC News*, June 19, 2017, retrieved June 6, 2018, <https://www.bbc.com/news/world-40321287>.
  59. "Figures at a Glance," United Nations Human Rights Commission, n.d., retrieved June 6, 2018, <http://www.unhcr.org/en-au/figures-at-a-glance.html>.
  60. "Statelessness," US Department of State, n.d., retrieved June 6, 2018, <https://www.state.gov/j/prm/policyissues/issues/c50242.htm>.
  61. Issie Lapowsky, "Trump Can't Block Critics on Twitter. Here's What This Means for You," *WIRED*, May 23, 2018, retrieved June 10, 2018, <https://www.wired.com/story/>

- donald-trump-blocking-on-twitter-unconstitutional/.
62. Masha Gessen, "'The Right to Have Rights' and the Plight of the Stateless," *New Yorker*, May 3, 2018, retrieved July 2, 2019, <https://www.newyorker.com/news/our-columnists/the-right-to-have-rights-and-the-plight-of-the-stateless>.
  63. "The Meditation Room at United Nations Headquarters (1952)," United Nations Multimedia, n.d., retrieved August 19, 2018, <https://www.unmultimedia.org/s/photo/detail/498/0049835.html>.
  64. "Dag Hammarskjöld: 'A Room of Light,'" United Nations, n.d., retrieved July 26, 2019, <http://www.un.org/depts/dhl/dag/meditationroom.htm>.
  65. "Dag Hammarskjöld Designs United Nations Meditation Room," Read the Spirit, n.d., retrieved June 27, 2019, <https://www.readthespirit.com/explore/dag-hammarskjolds-introduction-to-the-united-nations-meditaiton-room/>.

### CONCLUSION: THE NET STATE PATTERN

1. "Declassified Letter from N. Khrushchev to J. Kennedy," NSA Archive, George Washington University, October 24, 1962, retrieved September 21, 2018, <https://nsarchive2.gwu.edu/IMG/cmc1ltr.pdf>.
2. "The Cuban Missile Crisis, October 1962," Office of the Historian, US Department of State, n.d., retrieved September 21, 2018, <https://history.state.gov/milestones/1961-1968/cuban-missile-crisis>.
3. "Washington-Moscow Hotline," Cryptomuseum, n.d., retrieved September 21, 2018, <http://www.cryptomuseum.com/crypto/hotline/index.htm>.
4. "The Washington-Moscow Hotline," Electrospace, October 28, 2012, retrieved September 21, 2018, <https://electrospace.blogspot.com/2012/10/the-washington-moscow-hot-line.html>.
5. David Vergun, "Hotline, Now 50 Years Old, Continues to Promote Dialog with Russians," Army News Service, August 26, 2013, retrieved September 16, 2018, [https://www.army.mil/article/109986/Hotline\\_\\_now\\_50\\_years\\_old\\_\\_continues\\_to\\_promote\\_dialog\\_with\\_Russians/](https://www.army.mil/article/109986/Hotline__now_50_years_old__continues_to_promote_dialog_with_Russians/).
6. Allan Pease, "The Definitive Book of Body Language," *New York Times*, September 24, 2006, retrieved September 21, 2018, <https://www.nytimes.com/2006/09/24/books/chapters/0924-1st-peas.html>.
7. Alvin Snyder, "More History on a Murrow Obsession," USC Center on Public Diplomacy, July 28, 2009, retrieved July 2, 2019, <https://www.uscpublicdiplomacy.org/blog/more-history-murrow-obsession>.
8. Sean Hollister, "Here's How Facebook Defines Terrorism—and How It's Responding," *CNET*, April 23, 2018, retrieved August 26, 2018, <https://www.cnet.com/news/facebook-shares-terrorism-definition-al-qaeda-isis/>; Paul Cruikshank, "A View from the CT Foxhole: An Interview with Brian Fishman, Counterterrorism Policy Manager, Facebook," Combating Terrorism Center, West Point, September 2017, retrieved August 26, 2018, <https://ctc.usma.edu/a-view-from-the-ct-foxhole-an-interview-with-brian-fishman-counterterrorism-policy-manager-facebook/>.
9. Curt Mills, "Facebook Is Looking for a Counterterrorism Analyst," *US News & World Report*, November 14, 2016, retrieved August 26, 2018, <https://www.usnews.com/news/national-news/articles/2016-11-14/facebook-is-looking-for-a-counterterrorism-analyst>.
10. "Partnering to Help Curb Spread of Online Terrorist Content," *Facebook Newsroom*, December 5, 2016, retrieved August 26, 2018, <https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/>.
11. "Global Internet Forum to Counter Terrorism," *Twitter Blog*, June 26, 2017, retrieved August 26, 2018, [https://blog.twitter.com/official/en\\_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html](https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html).
12. Sheera Frenkel and Matthew Rosenberg, "Top Tech Companies Met with Intelligence

- Officials to Discuss Midterms,” *New York Times*, June 25, 2018, retrieved August 26, 2018, <https://www.nytimes.com/2018/06/25/technology/tech-meeting-midterm-elections.html>.
13. Kevin Collier, “Tech Companies Are Gathering for a Secret Meeting to Prepare a 2018 Election Strategy,” *Buzzfeed News*, August 23, 2018, retrieved August 26, 2018, <https://www.buzzfeednews.com/article/kevincollier/tech-companies-are-gathering-for-a-secret-meeting-to>.
  14. Rana Dasgupta, “The Demise of the Nation State,” *Guardian*, April 5, 2018, retrieved August 26, 2018, <https://www.theguardian.com/news/2018/apr/05/demise-of-the-nation-state-rana-dasgupta>.
  15. Alex Tabarrok, “The Case for Getting Rid of Borders—Completely,” *Atlantic*, October 10, 2015, retrieved August 26, 2018, <https://www.theatlantic.com/business/archive/2015/10/get-rid-borders-completely/409501/>.
  16. “From Thomas Jefferson to Benjamin Rush, 23 September 1800,” National Archives, n.d., retrieved August 17, 2018, <https://founders.archives.gov/documents/Jefferson/01-32-02-0102>.
  17. James Madison, “The Federalist Papers, No. 46 (The Influence of the State and Federal Governments Compared),” Constitution (website), January 29, 1788, retrieved August 17, 2018, <http://www.constitution.org/fed/federa46.htm>.
  18. Nelson Lund and Adam Winkler, “Common Interpretation: The Second Amendment,” Constitution Center, n.d., retrieved August 17, 2018, <https://constitutioncenter.org/interactive-constitution/amendments/amendment-ii>.
  19. James Madison, “The Federalist Papers, No. 51 (The Structure of the Government Must Furnish the Proper Checks and Balances Between the Different Departments),” Constitution (website), February 6, 1788, retrieved August 17, 2018, <http://www.constitution.org/fed/federa51.htm>.
  20. G. A. Almond, “Political Theory and Political Science,” *American Political Science Review* 60, no. 4 (1966): 869–79.
  21. Abigail Geiger, “How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks,” Pew Research Center: Fact Tank, June 4, 2018, retrieved August 17, 2018, <http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/>.
  22. “America in Crisis,” Edelman, January 21, 2018, retrieved August 17, 2018, <https://www.edelman.com/post/america-in-crisis>.
  23. James Madison, “Selected Quotes of James Madison,” Constitution Society, n.d., retrieved June 27, 2019, [https://www.constitution.org/jm/jm\\_quotes.htm](https://www.constitution.org/jm/jm_quotes.htm).
  24. James Madison, “Founders Online: From James Madison to Thomas Jefferson, 13 May 1798,” National Archives, May 13, 1798, retrieved June 27, 2019, <https://founders.archives.gov/documents/Madison/01-17-02-0088>.
  25. “America’s Wars,” US Department of Veterans’ Affairs, n.d., retrieved August 17, 2018, [https://www.va.gov/opa/publications/factsheets/fs\\_americas\\_wars.pdf](https://www.va.gov/opa/publications/factsheets/fs_americas_wars.pdf); Ai Lei Tao, “Nation-State Actors Responsible for Most Cyber Attacks,” *Computer Weekly*, September 22, 2017, retrieved August 17, 2018, <https://www.computerweekly.com/news/450426775/Nation-state-actors-responsible-for-most-cyber-attacks>.
  26. *Encyclopædia Britannica Online*, s.v. “Widmanstätten Pattern,” April 9, 2012, retrieved June 27, 2019, [www.britannica.com/topic/Widmanstatten-pattern](http://www.britannica.com/topic/Widmanstatten-pattern).
  27. Vagn Fabritius Buchwald, *Iron and Steel in Ancient Times* (Copenhagen: Det Kongelige Danske Videnskabernes Selskab, 2005), 26.
  28. Alice Walker, as quoted in William P. Martin, *The Best Liberal Quotes Ever: Why the Left Is Right* (Naperville, IL: Sourcebooks, 2004).