CONTENTS

Introduction

THE BATTLE

In early 2010, at a café in the eastern part of Turkey, a young man (I'll call him Ali) told me of his escape from Iran. Ali had been arrested the previous summer during the Green Movement, a series of popular protests that erupted after what many Iranians regarded as a fraudulent presidential election. As Ali sat on the sidewalk with his wrists tied, anticipating being picked up by police and pondering his fate, a local woman happened to drive by. She stopped her car, courageously whisked him away, and dropped him off at home. Despite this brief reprieve, Ali knew that the Basiji, part of the infamous Islamic Revolutionary Guard Corps, would soon be knocking on the door of his parents' place, and he decided to flee to a remote area in the north where his family owned a small plot of land.

Ali was one of millions of Iranians who challenged Mahmoud Ahmadinejad's victory in the presidential election that summer. On June 20, 2009, one of these brave demonstrators, Neda Agha-Soltan, was killed by a sniper. Her death came quickly as she sank down to the pavement, blood running from her mouth, people around her screaming in horror.[1] We know this because, unlike many of the brutal incidents that authoritarian regimes carry out in dark

prison cells, Neda's death was captured on a bystander's cell phone. Videos of this and other state violence against peaceful protesters were shared around the world, fueling outrage and condemnation. Green Movement demonstrators posted their eyewitness accounts on social media with the hashtag #iranelection, allowing the entire world to witness a revolution unfolding in one of the most repressive countries on the planet.

The role of social media (specifically, Facebook, Twitter, and YouTube) and the use of technology (cell phones and internet connections) quickly became a defining theme in how journalists and politicians around the world understood the protests in Iran. These platforms were filling an important gap left by the Iranian regime's press crackdown. A few days after the protests started, in a desperate move to regain control, authorities banned journalists from doing any street reporting.[2] Ahmadinejad closed twelve newspapers and locked up over one hundred journalists.[3] Twitter (now known as X) emerged as the main platform for citizens to transmit information about the protests and the government's violence. As a result, some even called the Green Movement a "Twitter Revolution."[4] There was a widespread sense of hope about the democratizing potential of these nascent technologies; beyond using social media and cell phones to document and share human rights abuses, activists could also use them to coordinate actions and mobilize their movement. The administration of U.S. president Barack Obama even asked Twitter to delay a planned systems update to avoid temporarily disabling access for protesters in Iran.[5]

This hopefulness about technology as a partner in liberation was bolstered in 2010 as popular protests erupted in Tunisia and Egypt. When Egyptians revolted against the regime of President Hosni Mubarak, Western media proclaimed it a "Facebook revolution," in homage to the gigantic Facebook groups formed by youth protesters to coordinate the demonstrations.[6] Many believed that young people in the Middle East and North Africa would be better equipped to secure justice and rights with the help of U.S.-made technologies.

While Western media and policy circles excitedly buzzed about the democratizing potential of new technologies, the picture on the

ground in Cairo, Tehran, and Tunis was not as straightforward. As Iranian journalist Golnaz Esfandiari would later explain, activists typically used word of mouth, text messages, emails, and blog posts to organize protests rather than social media.[7]

Finally, as Ali himself would soon discover, cell phone technology exposed protesters to enormous risks. When he arrived at his hideout destination in the north of Iran, he called his mother to tell her he was safe. Her relief would not last long: Ali's phone signal was picked up by a nationwide monitoring network, and he was arrested soon thereafter, in the middle of nowhere. He ended up in the notorious Evin Prison, known for the brutal rape and torture of inmates.[8] After spending several dreadful months behind Evin's walls, he was able to escape during a furlough and eventually made his way to eastern Turkey. Yet even at the time of our meeting in early 2010, he still changed locations every day, since he knew that the Iranian security services were actively hunting down dissidents across the border.

Those who praised the democratizing possibilities of technology and social media platforms failed to appreciate that repressive authoritarian regimes could be tech-savvy too. In Iran, and later in Syria, state authorities tactically lifted bans on the use of internet services, only to later scan posts to incriminate the messengers. The same technologies that help detect spam assisted state militias with identifying authors of antiregime social media posts. Military intelligence services were able to use location services to spot a group of people gathering on a street corner—real-time information that can be very useful when looking to disperse crowds before they can form.

I was appalled by the suffering the Iranian protestors endured; Neda Agha-Soltan was only four years younger than I was at the time. Their courage also deeply inspired me. I had recently won an election for a seat in the European Parliament by criticizing the Dutch government, while people in Iran were being shot by theirs for doing the same. I felt shocked—not by the behavior of these repressive governments, from whom I expected little else, but by our own double standards. The monitoring and surveillance technology these regimes

were using came from Europe: Italian-made hacking systems were the technology of choice for the regime of Bashar al-Assad in Syria, while French technologies helped Muammar al-Gaddhafi in Libya and British systems facilitated the Mubarak regime in Egypt.[9]

Right when European governments were condemning the repression of people and their human rights, European companies were exporting sophisticated monitoring software to Middle Eastern rulers. As Nokia-Siemens Networks would admit in 2010, they sold cell phone surveillance technologies to the Iranian authorities that enabled them to track the protesters—people who were peacefully asking for freedoms that any European today takes for granted.[10] In a hearing before the Subcommittee on Human Rights of the European Parliament, Nokia-Siemens's head of marketing tried to distance the company from Iran's abuses, arguing that, ultimately, "people who use this technology to infringe human rights are responsible for their actions."[11] While this is obviously true—no one disputes that the Iranian government is responsible for its actions—this does not absolve the company of its moral obligation to avoid assisting a repressive government. Engineers of companies with such contracts would have traveled to Iran multiple times to train users or to repair surveillance systems, and they likely received additional pay for staffing a hardship post. Moreover, the human rights violations in Iran were well known and well documented even before the crackdown on protests began in 2009.

As a newly elected member of the European Parliament, I was incensed by Ali's story, as well as by the stories of the other Iranian refugees I met on my trip to Turkey. What meaning did European statements in support of human rights even have when global tools of repression were produced right here at home? These double standards became a galvanizing foundation for much of my work in public service. I would spend the next decade using every policy tool imaginable trying to stop what I then called "digital arms"—software that inevitably violates human rights and ends up harming innocent people.[12] Unfortunately, there is still much more work to be done. Today, newer versions of these commercial hacking systems have only grown in force and scale. Even worse, as I learned more about

the sprawling digital arms trade over the past decade, I realized that Iran's Green Movement was merely one battle in the war to protect democracy from technological overreach.

The Reveal

When the Pegasus Project released a series of articles about government espionage in the summer of 2021, the news filled me with a mix of horror and hope.[13] Pegasus is the flagship spyware product of NSO Group—an Israeli technology firm that holds the pole position in the billion-dollar global spyware market. Sold as a counterterrorism and crime-fighting solution all over the world, spyware often ends up being used like a privatized intelligence service to stalk and repress critical voices. The investigative journalists who worked as part of the Pegasus Project revealed NSO Group's hit list: over fifty thousand phone numbers of the potential targets that the organization had been hacking on behalf of their clients.[14] For many, the Pegasus Project displayed the deep impact of hacking and surveillance technologies for the first time.

The leaks revealed the existence of highly sophisticated surveillance and hacking systems that made the tracking and tracing of Ali in Iran look wildly outdated. Pegasus can transform a target's phone or laptop into a live surveillance tool by remotely turning on microphones and cameras without the user's knowledge. These "zero-click" attacks, as they are known, are highly effective because the targeted individual does not even have to click on an infected link or do anything themself for the infiltration to begin. Once NSO Group gains access, its customers can extract contacts, call logs, messages, photos, web browsing history, and settings, and they can gather information from popular communications and chat apps.[15] Unsurprisingly, authoritarian governments across the world have been keen customers. NSO Group was valued at $2.3 billion before the Pegasus Project put a critical spotlight on the company.[16]

Beyond revealing what the technology could do and who was targeted, the leaked documents also showed who was involved with NSO Group. Former officials from the Obama administration and the

French government, for instance, had taken lucrative roles as senior advisers with the company—even as the phones of the president of France, the editor in chief of the *Financial Times*, and Hungarian opposition leaders were breached and monitored.[17] Nokia-Siemens's facilitation of Ali's arrest and NSO Group's ongoing dealings with autocrats beg a question: Why wasn't more being done to stop the development and sale of these technologies by democratic governments from within whose borders these companies operated?

One reason, though far from the only one, is that for too long our political leaders have been in the grip of an overly optimistic and self-centered view of new technologies. The data-driven strategies that were part of the successful campaign of Barack Obama in 2008 generated off-the-charts excitement among elected officials the world over. Politicians were keen to embrace new ways to communicate with citizens and constituents. I know this firsthand because communicating on social media platforms certainly helped me win my seat to the European Parliament. As a newcomer on the political stage, I may have never reached potential voters had it not been for Facebook and Twitter. Once elected, these platforms also offered a helpful way to update people on activities that would not be reported in newspapers or TV news bulletins. In my early days in the European Parliament, technological disruption was largely seen as a positive development.

But even as more information about the true nature and shadow sides of these technologies was revealed, and as companies grew massively, public officials did little. By the time the Pegasus Project revelations made headlines in 2021, I had spent a decade fighting the spyware sector and the toxic industry still had not been brought to a halt. Yes, we managed to get the European Union (EU) to adopt export controls, restricting the overseas sales of surveillance tools, but imports and thus domestic use remained untouched.

Naively, I initially thought that my fellow political leaders were not taking action on tech regulation because they simply didn't understand these rapidly evolving technological systems operating below the radar. Though such ignorance may have played a contributing

role in their inaction, the primary reason was much more cynical: democratic governments wanted to deploy these technologies too, to spy on their own populations. At the time, Europeans were practically apoplectic over U.S. intelligence services snooping on European leaders, including German chancellor Angela Merkel.[18] The governments of EU member states pushed new legislation to protect people from falling prey to American surveillance practices. Yet despite these governments' very public outrage, their own police forces quietly procured sophisticated infiltration systems to go after criminals and terror suspects. To this day, few European government agencies will admit to using Pegasus or similar systems. Later, in 2022, additional significant cases of spyware abuse, including the hacking of opposition leaders, judges, and journalists by the governments of Greece, Poland, and Spain were revealed.[19] Researchers from the Carnegie Endowment for International Peace created an index showing that seventy-four governments had contracted with commercial firms to obtain spyware or digital forensics technology.[20] In my home country, freedom of information requests to Dutch police went unanswered, but sources told investigative journalist Huib Modderkolk that Pegasus was used to hack the devices of Ridouan Taghi, the country's most notorious fugitive Mafia boss.[21]

In the United States, broader awareness about mass surveillance practices of U.S. intelligence services hardly led to decisive legal change. A decade after Edward Snowden's revelations, journalists, parliamentarians, and citizens are still barely capable of bringing transparency to the procurement of tech systems and services by democratic governments. It is a vivid reminder of how 9/11 continues to cast a long shadow over security policy, leading to disastrous moral confusion. On the one hand, there is the illusion of a clear line between democratic countries and their enemies. In the name of security, illiberal surveillance practices continue to erode civil liberties at the heart of democratic societies. On the other hand, to my frustration, the plight of human rights defenders and journalists in the Global South—many of whom were first to have been targeted by Western-made spyware—generated too little urgency to address the issue.

The failure of the Green Movement in Iran, as well as the lack of proper policy responses by democratic governments, made something manifestly clear during my first year in office: if technology was to serve people and promote democracy as it promised, laws were needed to turn those hopes into realities and to guard against both corporate opportunism and authoritarian capture. Merely assuming that information and communication technology (ICT) would foster the spread of democracy was clearly a failed strategy. Defending and advancing democratic principles would require intentionally updating and creating laws to express, revive, and protect those principles from both external threats and threats within our own borders. Indeed, today's attacks on democracy do not come from just authoritarian states or a loss of trust in the democratic process. The gradual erosion of democracy in our time is being accelerated by the growing, unaccountable power of technology companies, of which NSO Group is only one, albeit extreme, example.

The Global Shift

The unaccountable power of technology companies and the threat that they pose to democracy are by now familiar refrains. The newspapers are littered daily with scandals that cover the latest revelation of problems at one or another social media platform, search engine, or retail platform. The purpose of this book is not to preach to the choir and rehash those stories, however significant and urgent they may be. Instead this book begins from the premise that these incidents point to systemic problems that need unpacking: the fact that our social, professional, and civil lives are increasingly digitized and, essentially, *all* aspects of digitization are in the hands of private companies; that certain technologies have inherently antidemocratic characteristics, while laws to protect democratic values and the rule of law are lagging; and that, most important, democratic governments' outsourcing of key functions has led to a hollowing out of governments' core capabilities. These systematic problems are now undermining the core principles of democracy: free and fair elections, the rule of law, the separation of powers, a well-informed

public debate, national security and the protection of civil liberties such as freedom of expression, the presumption of innocence, and the right to privacy. Undermining principles have practical consequences; as we'll see in the coming chapters, tech's metastatic and unchecked growth has resulted in real-world violence, instability, and division.

The digital revolution has seen private companies increasingly take on functions normally assumed by states, leading to a concerning erosion of agency and accountability. For instance, Elon Musk's Starlink satellites, which dominate satellite-based internet services worldwide, have military chiefs worried, and with good reason: in the middle of the Russian war of aggression, Musk personally denied a request from Ukraine to turn on Starlink near Crimea. The Ukrainian government would need the connectivity to launch surprise attacks on Russian occupying naval vessels. But Musk decided the risk of Russian retaliation in the form of a nuclear attack was too great—a significant political decision from a businessman, and one he had the power to make. On Twitter the billionaire bragged, "Between Tesla, Starlink and Twitter, I may have more real-time economic data in one head than anyone ever."[22] Governments are beginning to realize that the tech sector's outsize influence is a major problem. President Joe Biden admitted as much on August 25, 2021, after inviting tech CEOs to a White House summit on cybersecurity: "The reality is," he noted, "most of our critical infrastructure is owned and operated by the private sector."[23] The U.S. president, arguably the most powerful leader in the world, conceded that the government alone cannot protect the homeland, and it needs tech companies to lend a hand.

That private companies, rather than the government, are responsible for such basic tasks as protecting national security and gathering intelligence may not have sunk in with the general public quite yet. Without public outcry, the needed regulation, oversight, and accountability are not moving along at the necessary speed.

During my years in the European Parliament, I progressively came to see technology through the lens of power. Technology could help emancipate people and raise unheard voices, or it could

transform disruptors into monopolists who ruthlessly pursued efficiency, surveillance, scale, and profit. In either case, technology is not neutral. As I will elaborate in this book, systems are themselves designed with values built into them, even if that is unintended. Additionally, given that most technologies are developed by private companies, these technologies are ultimately deployed for profit maximization, and profit maximization incentives are often misaligned with what is best for society. Sam Altman's Worldcoin, for example, aspires to build a global identity database by asking people in developing countries to scan their irises, in return for a bit of cryptocurrency; the firm is either blind or completely cavalier to the risks of concentrating so much sensitive biometric data under one roof.[24] Social media platforms seek to extend online engagement time of their users with little concern for the negative effect on teenagers' mental health.[25] Tech firms and their products now also make potentially life-altering decisions. Commercial algorithms designate triage statuses in hospitals and analyze medical images.[26] All the while, democratically elected representatives remain in the dark about key details of how these products work, since independent research is often impossible. For too long, too much trust has been placed in tech companies without making sure that their technology operates within the parameters of the rule of law and supports democratic outcomes.

An abdication of responsibility on the part of democratically elected leaders is what led to Pegasus being used to track members of the opposition in Poland and what enabled the Iranian government's monitoring of Ali. Laws are not updated to ensure that digital means of repression or intrusion are banned in the way that physical means would be. For instance, a conventional raid of an opposition party politician's home would immediately set off alarm bells, yet when hacking tools are deployed, there is less clarity or concern over the same kind of digital "raid." The introduction of new technologies seems to blur lawmakers' vision; they cannot fathom that violations of fundamental rights—like privacy and free expression—in the digital world are just as grave, while at times they are made much more easily and can be more vast in scope. Corporate leaders and aspiring

autocrats alike take advantage of this situational blindness and push the boundaries of the law. As digitization progresses, we see a gradual shift in responsibility and power away from democratic leaders. This shift accelerates two trends: growing digital authoritarianism and a wholesale decline in democratic governance.

In comparison to the European and U.S. governments, who have largely allowed private tech companies to operate as they please, the Chinese Communist Party (CCP) has made sure that new technologies serve its political system and values. It has spent the last two decades deploying them toward its own political advantage. The artificial intelligence (AI) sector, for instance, is powered by the limitless data collected by the Chinese government, whose repressive practices are fueling innovations from facial recognition applications to new ways of influencing and controlling massive amounts of people. During the COVID-19 pandemic, tracking apps were mandatory in China and used to survey whether people stayed at home in quarantine.[27] Similarly, the state uses sophisticated monitoring methods to verify and incarcerate the Uyghur minority population, both developing and entrenching state power.[28]

It is a model that China eagerly exports through the Digital Silk Road, as well as its other development projects. By investing in infrastructure and offering cloud computing to other countries, China keeps them connected with their data and development. Egypt, for example, has relied heavily on Chinese investment to modernize its telecommunications infrastructure and even construct a new smart city. The North African country has now also adopted China's model of internet governance via a new cybercrime law, and Egyptian government officials routinely attend Beijing's censorship training.[29]

The strategic marriage of geopolitics and technology in China lays bare how far technology governance lags on the part of democratic countries, a discrepancy that not only impacts the citizens of those countries but also affects the ability of nations to come to shared rules and solutions. It is difficult for the United States to lead the international community toward consensus on robust technology regulations, for example, given its laissez-faire approach toward Silicon Valley. China offers a cohesive, top-down governance model,

ready to be copied. This mismatch further entrenches the agency of both corporate powers and authoritarian states.

The entangled nature of technology—linking economics, security, and rights—requires an integrated political vision. Yet democratic leaders have too often responded to disruptions with inaction or a piecemeal approach, and they struggle to articulate an alternative to the technology industry's preferred hands-off approach to regulation. Without a blueprint for how to enshrine democratic standards domestically, a credible foreign policy agenda is impossible. To rein in the outsize power of technology companies, regain control over their products' basic functions, and protect democratic values on the world stage, democratic countries need to develop more robust legal and governance frameworks, effective institutions, and strong incentives that avoid abuses of power on the part of states or companies using technologies.

The Task

Reinventing democratic governance to match the challenges of digitization will not be an easy task. Today's policy processes are running out of sync with the pace and scale of corporate operations. This mismatch is a growing problem for those who believe democracy should not be disrupted, no matter how exciting the shiny new objects from Bangalore, Shenzhen, or Silicon Valley might look. It means that democratic governance should be revived and updated.

During my time in office, the more I worked on technology-related issues, the clearer it became that there was a huge and growing gap between corporate power, on the one hand, and democratic regulatory and oversight capability, on the other. In some cases, this is mainly about money. As of January 2024, Apple had a market capitalization of $3 trillion, making it more valuable than the stock markets of Australia and Germany combined.[30] As a result of such resource disparity, the public sector has fallen so far behind the tech sector in innovative capabilities (not to mention salaries, computing power, knowledge, and talent) that its ability to set rules for and by the people is severely hampered.

In other cases, lawmakers' lack of access to information impedes evidence-based rulemaking. Software is complex: large legacy programs can have tens of millions of lines of code, and machine learning systems may develop rules that even their own creators do not completely grasp. Moreover, companies have learned to use intellectual property law to protect the opacity of proprietary algorithms and to shield their treasured workings behind trade secret protections. In general, existing legal protections, made in an era before the internet even existed, disproportionately benefit companies. The same laws that help Coca-Cola protect its secret recipe also protect technology firms from disclosing how their algorithms function.

Let's consider new challenges to the Freedom of Information Act (FOIA), which journalists use to uncover information about government services. When government services are outsourced to technology companies, FOIA requests regarding those services can be denied when companies invoke intellectual property protections or even privacy standards as an exception to providing openness and accountability. In other cases, government officials will simply not feel bound to preserve records when using private, nongovernmental channels of communication. For instance, the EU's ombudsman had to issue an official ruling to underline that text messages exchanged by EU leaders on WhatsApp are subject to record-keeping and transparency rules, just as official emails and letters are. Just months after its lobbying blitz, Mistral AI announced a partnership with Microsoft, further consolidating AI assets in Silicon Valley.[31]

In some cases, corporate reticence takes absurd forms, as I learned on a trip to Silicon Valley in 2016 with my European Parliament colleague Kaja Kallas, who has gone on to serve as the prime minister of Estonia. We were working on new legislation that concerned illegal speech on online platforms and traveled halfway around the world to meet with representatives of Facebook, Google, and Yahoo. At most companies, legal teams walked us through the company policies for dealing with illegal and harmful content and underlined how they worried about protecting freedom of expression. But our experience at 1 Hacker Way, Facebook's headquarters in Menlo Park, California, was altogether different. We began the day with a long tour of the

campus as guides steered us around like tourists at Disneyland, pointing out every piece of whimsical art and the all-you-can-eat cafeterias in the vast, multicolored office building. When we finally took our seats in a meeting room, our hosts broached a conversation about *Lean In,* the new and highly influential book from Facebook's then-COO, Sheryl Sandberg, that considered the gender-based challenges facing women in the workplace. The conversation might have been interesting for a weekend book club, but we had not come all this way to talk about *Lean In*. When we reminded our hosts that we were there to discuss what responsibility the social media platform had to moderate content uploaded by users, they responded with polite smiles and nods: "Oh, we are terribly sorry, but for that subject you would need to talk to our legal team," to which we replied, "Well exactly, that is why we are here." Unfortunately, we were told, the people with expertise and authority to speak with us were not available.

This visit, peculiar in its own right, also spoke to a far more fascinating dynamic in Silicon Valley. Corporate giants did not feel accountable to lawmakers like me. They thought that they could dodge real policy and enforcement questions with free frozen yogurt and inspirational buzzwords—and we hadn't yet proven them wrong. As democratic governance long failed to impose guardrails on companies like Facebook, they had grown to believe that they operated above the law.

The Delivery

In 2019, after serving more than a decade in the European Parliament, I stepped down from politics and moved to the belly of the beast: Silicon Valley and Stanford University. I wanted to help bridge the gaps between the worlds of politics, policy, and technology.

Not long after I arrived at Stanford, I attended a presentation that confirmed just how badly such bridges were needed. The speaker, an engineer who had just left Instagram, shared fascinating experiences about curation of content through algorithms and how taste and culture could be shaped by decisions of what photos were posted on the front page of a user's feed. In other words, technology could be used to shape behavior and consumption. The engineer then discussed

how this allowed companies of a certain size to move and affect markets. By putting a post of a celebrity with a cosmetics product on the homepage, the company significantly increased the likelihood that the product would see an uptick in sales.

When the time came for questions, I took the microphone. Did that ability to move and create markets, I asked, also imply the possibility of influencing, shaping, or moving political beliefs, values, and behavior more widely? Could it also move masses? A popular meme ridiculing a candidate in a political race, a call by a popular influencer to go shopping instead of voting on Election Day, or the sale of merchandise from the Black Lives Matter movement or the National Rifle Association, for instance, could be increasingly powerful if their reach was amplified. As it is not always easy to define clearly what qualifies as political content online, I wanted to know about the discussions among engineers and whether the societal or political impacts were ever considered when designing recommendation algorithms that cater to billions of people. The engineer admitted that they did not understand the question. In a way, that was the clearest answer I could have asked for.

The fulfillment of the democratic promise by politicians and states has never been perfect. But the Churchillian adage, that democracy is the worst form of government except for all others, still holds. We must preserve democracy, and to do that, our governments must regain control over our society's technological capabilities. While there are some encouraging signs in terms of new laws, regulatory proposals, and citizen initiatives, they remain too slow and ad hoc to truly shift the status quo and restore the balance of power between public authorities and private companies. These alone won't stop the privatization of the entire digital sphere. While many like to contrast the EU's and the United States' different legal and political cultures, I prefer to emphasize the unfortunate paralysis and tendency toward inaction that they have in common. The entire democratic world has been too slow to build a democratic governance model for technologies, and countries have not done so together. Ash Carter, the late former U.S. secretary of defense, lamented the "ethos of public purpose that has become dangerously decoupled from many of today's leading tech endeavors."[32] I agree.

Democracy is not flawless, nor does it claim to be. What the political system possesses, however, is the ability to improve. As Samantha Power explains, "Democracy wins out in the long run because it offers a chance to fix its own mistakes. It is the only system built on the premise that if something is not working, people can actually correct it, from the bottom up. Democracy works best when people are given the opportunity to constantly monitor and repair the kinks in the machinery."[33] At its best, democracy is deliberate, self-correcting, and compromise-generating. It is never static but is a process in motion. And that should give us hope for its future.

It is time to normalize the way we think about updating laws and adopting regulations to match the power of technology companies. To understand what this could look like, we can look to another tool that saw exponential growth over the past century: cars. People and governments are aware of the benefits of cars. But it would have been shortsighted if, out of fear of stifling automobile growth, governments refrained from requiring driver's licenses, imposing safety regulations, or addressing the environmental harms and other negative externalities produced by driving. Moreover, when a particular model of car systematically breaks down, no one expects individual drivers to take responsibility. No one believes that merely by starting the engine, the driver has agreed to accept any underlying flaws or dangers in the car's design. No one would believe a simple statement by the car manufacturer that the car is safe, environmentally friendly, and energy efficient. All these elements, standards, and commitments are independently tested to make sure that people are safe and the environmental damage is limited. Companies are not blindly trusted to preserve the public interest, and when corporate leaders violate these standards—for instance, as when Volkswagen lied about emissions while tampering with emissions software—parliamentary inquiries seek to bring accountability. Even though cars are complex technologies, rules about their qualifications were put in place and guardrails around their use adopted. Doing the same for digital technologies is both urgently needed and practically possible.

The history of the car's influence on society also offers another important lesson for the task we confront in this book. Today we

have huge roads, bridges, and parking structures; we have enormous factories for the production of cars; natural resources are drilled and burned to ensure that cars can be driven; and we have traffic rules that apply on public roads. All this existing infrastructure is difficult to reverse or ignore. The same will happen with digital infrastructure soon enough, and the laws we adopt today will determine the path of emerging technologies and the trajectory of their associated infrastructure. We must act wisely. Without rules to protect people's safety, to regulate behavior in public spaces, or to ensure that companies are doing as they say and saying as they do, the harm to society and indeed to democracy will be significant.

This is a book about the impact of digital disruption on democracy. This is, of course, far from the only problem with the tech industry. However, I am choosing a focused lens here, as I am convinced that a loss of insight, agency, and oversight on the part of citizens and public institutions cannot be compensated for with the exciting perspectives of economic growth or innovation benefits. I am not under the illusion that technology can be stopped. It should not be, and I am hopeful and excited about what technology can continue to bring to us all. Yet I am very critical of a powerful, unaccountable industry that, to date, has been almost entirely without guidance or guardrails from democratic authorities. Solving the accountability gap is particularly urgent because technology is not a sector but a layer that impacts almost all sectors.

In Support of Democracy

This is not a book against technology but in favor of democracy. It is a call to rebalance technology's role in democratic societies to ensure better protection of democratic values. It urges democratic governments to safeguard the public sphere, to develop future-proof solutions, and to revive and reinvent its approach to tech regulation, knowing that new technologies will continue to challenge and disrupt. We do not have time to address these harms in an ad hoc manner: endlessly debating whether Facebook's community standards are helpful or not shifts our attention away from broader and more

systemic issues. A new approach to tech policy needs to be holistic, looking at the bigger picture and always in service of strengthening democratic principles. In other words, it is time to tackle the causes, not the symptoms.

The Tech Coup shifts the spotlight from Big Tech's scandals to the systematic erosion of democracy as private companies run ever more parts of our digital lives. You, as a democratic citizen, are invited to help shape an agenda that puts the survival of democratic principles ahead of short-term economic benefits. States can remain very powerful actors if they choose to be, as unfortunately illustrated by the bitter success of authoritarian models of governing in the digital world. Revitalizing democracy will require new approaches to lawmaking and innovative forms of governance designed to explicitly support democratic principles in new contexts. And it will demand that we craft and enforce policies that better equip democracy for surviving the twenty-first century. While technological fixes are necessary, they alone are insufficient, and for any of them to work, we need a broader, functional political infrastructure to serve the people.

Restoring democratic governance over technological systems—instead of allowing privatized governance over our digital world—will go a long way toward making the world a more fair, just, and equitable place.

INDEX