

CONSENT | OF THE | **NETWORKED**

The Worldwide Struggle
for Internet Freedom

REBECCA MacKINNON

2012

BASIC BOOKS

A Member of the Perseus Books Group

PREFACE

One night in Beijing in 1998, I went to dinner with a few Chinese friends—all artsy intellectuals, journalists, and hip liberal types. As we dug into a mound of spicy Szechuan chicken and washed it down with lukewarm local beer, I described a book I had just finished reading: *The File* by Oxford historian Timothy Garton Ash. It tells the story of how after the Berlin Wall came down and the Iron Curtain crumbled, East Germans suddenly had access to the files the Stasi had been keeping on them. People found out who had been ratting on whom—in some cases neighbors and coworkers, but also lovers, spouses, and even sometimes their own children.

After I finished talking, one friend put down his chopsticks, looked around the table, and proclaimed, “Someday the same thing will happen in China. Then I’ll know who my real friends are.” The table fell silent.

If and when China does change, that day of reckoning may never come. In the age of broadband and smart phones, state security agents no longer depend so heavily on human informants. Not only are software and hardware more efficient and omniscient than humans, but conveniently they also lack consciences.

As a Beijing-based journalist working for CNN from 1992 to 2001, I found the Internet’s arrival to be tremendously exciting. Most Western journalists and diplomats in China at the time assumed that the Communist Party’s grip on power could never survive this new globally networked technology. A decade later, after leaving TV journalism and becoming an independent writer, researcher, and activist, I grew to

realize that we were naive. Though the Internet has transformed Chinese society in many ways, the regime has also succeeded in adopting technology to its advantage in ways I had not imagined—ways I have spent much time over the past several years trying to understand.

After I left China in 2001 and moved to Japan as CNN's Tokyo bureau chief, my fascination with the Internet's effect on global politics broadened. On a trip to South Korea, I reported on how Roh Moo-hyun won the presidency in December 2002 by a narrow margin thanks to eleventh-hour online and mobile activism by readers of OhMyNews, one of the world's first online citizen journalism ventures. In January 2003 a friend introduced me to "Where is Raed?" the blog of an Iraqi man in Baghdad writing under the pseudonym Salam Pax. As the United States and its allies prepared to invade, he ranted cynically against Saddam Hussein's regime, the Bush administration, and almost everyone and everything else. As the web publishing magnate Nick Denton aptly put it, he was the "Anne Frank of the war . . . and its Elvis." As I started following blogs written by other less famous but no less eloquent people all over the world—people who were not professional journalists but who were witnesses or parties to events that no mainstream Western news media had reported—it was clear that the Internet-driven citizen media revolution had implications not only for the future of journalism but also for geopolitics.

In January 2004 I took what was supposed to have been five months' leave from CNN's Tokyo bureau to spend a semester at the Shorenstein Center on the Press, Politics, and Public Policy at Harvard's Kennedy School of Government, where I made it my full-time job to learn about the new world of citizen-driven online media. I started blogging. A couple of months into my leave, I decided to stay at Harvard and not to return to CNN. I moved to a new think tank called the Berkman Center for Internet and Society, the epicenter of new thinking and experimentation on citizen media and networked politics.

To keep my Chinese from getting too rusty, I began to follow Chinese blogs. Reading bloggers' observations, musings, and conversations helped me to keep up with events, cultural trends, and controversies in

China in a way that would have been impossible without the Internet. As it so happened, another colleague, Ethan Zuckerman, closely followed blogs from Africa and the Middle East. Ethan and I started to think about how we might support and amplify the work of bloggers who write about events in their countries, sharing insights and information not reported in the mainstream media. At the end of 2004 we organized a brainstorming meeting of bloggers from all over the world and called it Global Voices Online.

The discussions that day inspired our group to build an online community to help promote and support the work of civic-minded bloggers around the world. A conference blog evolved into a complex website. Today Global Voices is a full-blown nonprofit organization. Bloggers living all over the world work to curate, explain, summarize, and translate postings related to current events on blogs and other social media like Facebook, Twitter, and YouTube. Another team gives small grants to citizen media projects in the developing world. Yet another team translates Global Voices content back and forth across roughly two dozen languages. Last but not least, our activist team runs a network devoted to raising awareness about threats to online free expression and assembly, helping people navigate censorship and protect themselves against surveillance. As protests erupted in Tunisia in late 2010 and demonstrations spread around the Middle East and North Africa in early 2011, Global Voices contributors worked around the clock to spread information about what was happening in multiple languages, on our own site as well as Twitter, Facebook, and other social media platforms.

As Global Voices grew, I continued to follow the evolution of Chinese blogs and social media, returning regularly to China to attend blogger gatherings and getting to know some of China's boldest online activists. I also began to research China's Internet censorship system. Other researchers had begun to study China's "great firewall"—the system by which a large number of overseas websites are blocked from view on the Chinese Internet. I soon realized, however, that website blocking was just one part of the Chinese government's strategy to control

the online activities of Chinese citizens. A core component of that strategy involves censorship and surveillance carried out not by government agents or "Internet police" but by the private sector. After Yahoo, Microsoft, Cisco, and Google came under fire at a 2006 congressional hearing for their role in Chinese censorship and surveillance, I began to be asked regularly to write and speak about the problem of corporate collaboration in Chinese censorship and surveillance. I joined a group of Internet companies, human rights organizations, socially responsible investors, and academics who together in 2008 launched the Global Network Initiative, an organization that has established standards for free expression and privacy for the Internet and telecommunications sector, to which it seeks to hold companies accountable.

Five years ago when I first considered writing a book, I was inclined to focus on China as "exhibit A" for how an authoritarian regime can not only survive, but also thrive in the Internet age with the help of domestic and multinational corporations. My experience with Global Voices and as an advocate for online free speech on an international scale, however, has also taught me that the root causes are broader. The technologies and policies that make surveillance and censorship possible in China and many other countries are closely connected to policy, business, and technical decisions being made by governments and companies in the democratic West. Sometimes those decisions are made by people who understand the implications of their actions but simply have other priorities. Others have good intentions but are ill-informed about the dynamics of power, control, and freedom across a global Internet.

In mid-August 2011, as I completed the final edits on this book, riots broke out in Great Britain. Debates raged in the United Kingdom over Prime Minister David Cameron's controversial remarks about the need for expanded government power to monitor and restrict the British public's access to mobile services as well as to social networks. In the United States, San Franciscans were up in arms after the local subway system, Bay Area Rapid Transit (BART), shut down wireless service at several stations to prevent a planned protest against a shooting by BART police of an allegedly knife-wielding man. China's state-run

Xinhua News Agency could not resist the opportunity to gloat: "We may wonder why Western leaders, on the one hand, tend to indiscriminately accuse other nations of monitoring, but on the other take for granted their steps to monitor and control the Internet," said the unsigned commentary. "For the benefit of the general public, proper Web monitoring is legitimate and necessary."

I am concerned about what will happen to the Internet—and more broadly to the future of freedom in the Internet age—if the world's democracies develop a habit of tackling problems in a short-sighted, knee-jerk manner, without considering the long-term domestic and global consequences. This book is thus a distillation of what I have learned over the past decade about the global struggle for Internet freedom and an attempt to apply those learnings to our common future. It is an effort to crystallize what worries me most—and to galvanize others to defend individual rights that are under threat, on a scale and in ways that are only beginning to become apparent. I worry that the future of freedom and democracy in the Internet age will not be as bright as many assume. Yet I am also hopeful: I have had the privilege to work with innovative and often very brave people from all over the world who are using technology to speak truth to power and to give voice to their communities and fellow citizens.

Many of these people are fighting uphill battles just to be able to keep using technology to express themselves and organize peacefully without censorship or fear of reprisal. The obstacles to their success are created not only by authoritarian governments, but also by Western companies and democratically elected politicians who do not understand the global impact of their actions—or, more ominously, do not care. This book is my effort to raise the level of public awareness about the many inconvenient truths of the Internet age. I have sought to explain what I believe all citizens everywhere need to know about the global struggle for Internet freedom. The outcome of this struggle will affect each and every one of us. It is a struggle that all of us have the power and ability to influence—even in small ways—if we understand the complex forces at work and how we might shape them.

Entire books have been written about many of the issues raised in each chapter. I have listed some of them in the endnotes for readers who want to go deeper. My aim here is to tie together the broader set of overlapping, complex issues in a way that makes sense to an informed reader who does not have special Internet-related expertise—beyond simply being an Internet and cell phone user. For people who are experts on some of these issues, I have tried to provide a fresh conceptual framework and geopolitical context, which I hope will be useful to experts and nonexperts alike who are concerned about the future of freedom in the Internet age.

It is not possible to document in one concise book all the violations of Internet freedoms and rights happening everywhere in the world. If your rights to digital free expression and assembly are under attack but your country is not mentioned in this book, please understand that the omission does not imply a lack of concern for the violations you and your compatriots are enduring. Several organizations, including the Open Net Initiative and Freedom House, produce regular reports systematically documenting attacks on Internet freedom, country by country. Nor is it possible in one book to catalog every violation of free speech and privacy by every company everywhere. I have selected specific examples that best support the overall argument. Please see the book's companion website at www.consentofthenetworked.com for further sources of information and links to organizations that document ongoing cases.

I am not able to list here all of the people who made this book possible—or who taught me what I needed to know to write it. Beyond the obvious reasons to thank my parents, I also owe most of the credit for my fluency in Chinese, lifelong connection to China, and broader fascination with global politics to Stephen R. MacKinnon, professor of modern Chinese history, and the late Janice R. MacKinnon. In 1979 my parents took my mother, Cyrus, and me to live in Beijing for two years, enrolling us in a Chinese primary school, so they could conduct research on a book. None of us realized at the time what a gift they had given their children.

More than two decades later when I was working as a foreign correspondent in Tokyo, I met Joi Ito, who introduced me to blogs, catalyzing a chain of discoveries and friendships that ultimately propelled me away from conventional journalism and down the winding path I have taken. Adam Greenfield jolted me out of my TV reporter's mindset and challenged me to think in new dimensions. My dear friend and colleague Ethan Zuckerman has been a rock since we started collaborating in 2004, providing critical support and substantive advice as this project evolved. Harvard's Berkman Center for Internet and Society is a truly unique intellectual launching pad and support system from which I continue to benefit in delightfully random ways. In 2007 and 2008, Ying Chan at Hong Kong University's Journalism and Media Studies Centre took me in and supported my controversial research and unorthodox projects.

A generous fellowship from the Open Society Foundations in 2009 supported research and travel that enabled me to figure out what this book really needed to be about. Without subsequent fellowships from Princeton's Center for Information Technology Policy and the New America Foundation in Washington, DC, I could not have afforded the time and head space that completion of this project demanded. At various points along the way, friends and colleagues gave me ideas that I have incorporated. Notably, "digital bonapartism" came from the great brain of Yale historian Timothy Snyder. Joshua Cooper Ramo and Kathy Robbins offered game-changing reactions to early versions of the book proposal. Family and friends lent guest bedrooms, proffered food and drink, and provided moral and emotional support throughout my nomadic research and writing phase. Henrik Bork and Wang Kuangyi were especially generous with their Beijing apartment. Most profoundly, the Global Voices community schooled me daily, giving me a faith in humanity that I might otherwise have been hard-pressed to retain.

It has been a delight and an honor to be represented by John Brockman, visionary curator of ideas and convener of people working at the intersection of science, technology, and society. He grasped what I was trying to do before I completely understood it myself, challenged me to

focus and refine my argument, and made it possible for Max Brockman to deploy his literary matchmaking talents. I am eternally thankful to TJ Kelleher at Basic Books for believing in me, and for guiding me through the muddy waters of rough drafts and uncertainty as a first-time book author. Special gratitude goes to Ethan Zuckerman, Maya Alexandri, Ian Johnson, Tom Glaisyer, Ivan Sigal, David Sasaki, Luisetta Mudie, Mary Kay Magistad, Anna Husarska, and my father, Stephen MacKinnon, who volunteered precious time to read drafts and comment. Finally, I have no idea how I would have held on to my sanity in the process of intense writing, editing, and rewriting without the support—editorial and emotional—of my loving partner and intellectual muse, Bennett Freeman.

August 2011
Washington, DC

INTRODUCTION

After the Revolution

On March 5, 2011, protesters stormed the Egyptian state security headquarters. In real time on Twitter, activists shared their discoveries with the world as they moved through a building that had until recently been one of the Mubarak regime's largest torture facilities. Videos and photos uploaded to YouTube, Flickr, and Facebook showed a flurry of young men (and a few women) opening doors and cabinets, sifting through piles of shredded paper, pulling out stacks of files, and examining pieces of equipment. Some were implements of torture.

"Entered the small compound where I was locked," tweeted Hossam el-Hamalawy, a thirty-three-year-old journalist and activist who had been detained and tortured several times since they first picked him up as a student activist thirteen years ago. Returning home a few hours later, he told his followers, "I've been crying hysterically today."

Some activists found their own files. They were full of wiretap transcripts, reams of printouts of intercepted e-mails and mobile messages. All kinds of records had been kept about them: lurid details of divorces and personal relationships; all their past job applications; foreign organizations they had communicated with; international meetings they had attended. Clearly the Egyptian government had sophisticated surveillance technology at its disposal. It still does.

Wael Ghonim, the young Google executive and a hero of the Egyptian revolution for his role in creating and running the Facebook protest group that played a key role in getting the first wave of protesters into

Cairo's Tahrir Square, famously told CNN, "If you want to liberate a society just give them the Internet." The Internet certainly did play a powerful role in bringing down a dictator—the Internet in the hands of a committed community of activists who spent the better part of a decade building a movement. It is less clear how helpful the Internet will be when it comes to protecting the Egyptian people's rights in the post-Mubarak era and in building a new democracy.

If the events of 2011 taught the world anything, it is that although the Internet empowers dissent and activism, it is not an instant freedom tonic that, when applied in sufficient quantities, automatically results in freedom. It is time to stop debating *whether* the Internet is an effective tool for political expression, and to move on to the much more urgent question of *how* digital technology can be structured, governed, and used to maximize the good it can do in the world, and minimize the evil.

Even if Egypt does manage to establish a stable democracy, the Egyptian people face a problem that none of the world's democracies have yet solved: How do we make sure that people with power over our digital lives will not abuse that power?

In mature democracies, laws and regulations governing digital platforms and networks arguably represent "consent of the governed"—to the extent that political traditions and institutions reflect the will of the people as a whole, as distinct from representing mainly special interest groups, corporate lobbies, and the loudest and most extreme elements of both political parties. Of course, the extent to which democratic politics in the United States, United Kingdom, and other democracies around the world actually succeed in accomplishing the former rather than the latter is a matter of fierce debate.

Americans across the political spectrum continue to have real and legitimate concerns that the system—the political process, media organizations, and information networks—is vulnerable to capture, manipulation, and abuse. There is good reason to worry about the way in which our digital lives are being shaped by regulators, politicians serv-

ing powerful constituencies, and companies seeking to maximize profit. The potential for manipulation and abuse of the digital networks and platforms that citizens have come to depend upon is one of the more insidious threats to democracy in the Internet age. If citizens of established democracies cannot prevent such manipulation, the prospects for aspiring and fragile democracies in Tunisia and Egypt, let alone hopes for the future in places like Iran and China, look much less bright.

It is a reality of human nature that those with power, however benign or even noble their intentions, will do what they can to keep it. The American revolutionaries certainly understood this truth. As James Madison, one of the framers of the Constitution, observed near the end of his life in an 1829 speech before the Virginia Constitutional Convention, "The essence of Government is power; and power, lodged as it must be in human hands, will ever be liable to abuse." This was their fundamental assumption as they formed new institutions of the world's first democratic republic.

In the physical world, mechanisms of democratic politics and constitutional law have worked—not perfectly, but still far better than any alternatives—to protect citizens' rights. But these mechanisms are no longer adequate for people whose physical lives now depend on what they can or cannot do (and what others can do to them) in the new digital spaces where sovereignty and power are ill-defined and highly contested. The reality is that the corporations and governments that build, operate, and govern cyberspace are not being held sufficiently accountable for their exercise of power over the lives and identities of people who use digital networks. They are sovereigns operating without the consent of the networked.

This absence of consent takes place on several levels. Governments are exercising power over people outside their jurisdictions through global Internet companies. When citizens depend on platforms like Google, Twitter, and Facebook, whose digital inhabitants include people from nearly everywhere on earth, legislators and regulators in the world's

largest markets make decisions that ultimately shape global technical standards and business norms. Thus governments are exerting power over the freedoms and rights of people who did not vote for them, who do not live under their jurisdiction, and who have no meaningful way of holding them accountable.

"Governance" functions, once carried out almost entirely by nation-states, are now shared increasingly by private networks and platforms. The lives of people around the world—from people living in democracies, such as the United States, to those living in authoritarian regimes, such as China—are increasingly shaped by programmers, engineers, and corporate executives for whom nobody ever voted and who are not accountable to the public interest in any way. When we sign up for web services, social networking platforms, broadband service, or mobile wireless networks, and we click "agree" to the terms of service, we give them false and uninformed consent to operate as they like.

Today the power of Internet platforms and services to shape people's lives is greater than ever and will only continue to grow. Though some Internet companies are helping to empower people in innovative and exhilarating ways, many are also helping authoritarian dictators adapt and survive in the Internet age. In China, Western companies and financiers have supported and helped to legitimize a political innovation that I call "networked authoritarianism," in which corporate networks are turned into opaque and subtle but invasive extensions of government power. Leaders of stunted crypto-democracies like Russia have adopted what I call "digital bonapartism," using populist rhetoric, combined with control over private enterprise and the legal system, to marginalize the opposition and manipulate public opinion much more subtly than in the old days. Even theocratic dictatorships like Iran are using their control over networked technologies to serve their economies and improve governance while preventing opponents from successfully using the Internet to overthrow them.

Many corporate executives argue that human rights are neither their concern nor their responsibility: the main obligation of any business, they point out, is to maximize profit and investor returns. But what kind of world are they helping to create, and should that not concern them? In the first half of the twentieth century, corporations were forced to consider employees' safety and health. In the past fifty years the environmental movement has forced industry to share responsibility for pollution and more recently climate change—though they have not gone nearly far enough. So far, most Internet and telecommunications companies have failed to accept responsibility—beyond cyber-utopian platitudes—for the rights of their customers and users, even as companies in other, much older industries have long since begun to do so with their workers, shareholders, and broader stakeholders.

Building accountability into the fabric of cyberspace requires political innovation to match the rapid technical innovation of the forty-plus years since the Internet was invented. In the twenty-first century, many of the most acute political and geopolitical struggles will involve access to and control of information. Human freedom increasingly depends on who controls what we know and therefore how we understand our world. It depends on what information we are able to create and disseminate: what we can share; how we can share it; and with whom we can share it. It also depends on the extent to which we have any control—or any say in—how our own information is shared with other people, private companies, and governments.

This book is about the new realities of power, freedom, and control in the Internet age. People, governments, companies, and all kinds of groups are using the Internet to achieve all kinds of ends, including political ones. But we cannot understand how the Internet is used unless we first understand the ways in which the Internet *itself* has become a highly contested political space. Pitched battles are currently under way over not only who controls its future, but also over its very nature, which in turn will determine whom it most empowers in the long run—and who will be shut out.

Contrary to what some people may have hoped and believed, the Internet does not change human nature. We have begun to see how absolute power in cyberspace corrupts absolutely as it does in physical space. As with power in the physical world, power in the digital world must be constrained, balanced, and held accountable. The future of freedom in the Internet age depends on the choices and actions of everybody on the planet who creates, uses, and regulates technology. It depends on whether we assert our rights within the digital spaces we now inhabit—just as our forebears fought for their rights in the physical spaces once controlled entirely by sovereigns who claimed to have the divine right to rule as they pleased.

The first step toward engaging in this struggle is to understand how the dynamics of power and freedom have changed, now that our political lives have become highly dependent on digital services and platforms that are largely owned and operated by the private sector. Part One will explain how the Internet—driven by the private sector—has challenged the power and legitimacy of the nation-state, and has also given rise to a new digital “commons” that incubates much innovation as well as some of the world’s most disruptive digital activism. Part Two describes a phenomenon that some call “Control 2.0”: how opaque, unaccountable relationships with Internet and telecommunications companies enables authoritarian governments to control and manipulate citizens. Though China is the most advanced case, a range of other authoritarian regimes are also taking advantage of their power over private networks and platforms. Part Three examines how democracies are being corroded by increasingly opaque and unaccountable relationships between government and the companies that own and operate the digital networks and platforms upon which our democratic discourse increasingly depends. Part Four describes how companies act as the new sovereigns of cyberspace—and how most companies’ failure to take responsibility for their power over citizens’ political lives, and their lack of accountability in the exercise of that power, corrodes the Internet’s democratic potential in often subtle and

insidious ways. Finally, Part Five explores efforts by some governments, a few companies, and a growing number of concerned citizens to address the threats to freedom in cyberspace through new initiatives and movements.

The Internet is a human creation. Power struggles are an inevitable feature of human society. Democracy is about constraining power and holding it accountable. The Internet can be a powerful tool in the hands of citizens seeking to hold governments and corporations to account—but only if we keep the Internet itself open and free.

PART ONE

DISRUPTIONS

To no one will we sell, to no one will we
refuse or delay right of justice.

—MAGNA CARTA, 1215

CHAPTER 1

Consent and Sovereignty

On Super Bowl Sunday, January 22, 1984, Apple ran one of the most famous TV advertisements of all time. It opened with a gray theater full of people with shaved heads, wearing gray jumpsuits, staring expressionlessly at a large screen. From the screen, an Orwellian “Big Brother” intoned, “We are one people, one whim, one resolve, one course. Our enemies shall talk themselves to death, and we shall bury them with their own confusion. We shall prevail.” As he spoke, an athletic young blonde woman in a blinding-white tank top and bright orange running shorts ran into the theater and down the center aisle, carrying a sledgehammer. She threw it at the screen, and the screen exploded. An off-camera voice declared, “On January 24th, Apple Computer will introduce Macintosh. And you’ll see why 1984 won’t be like 1984.”

Today, more than two decades later, the message remains tremendously powerful: innovative technology in the hands of brave people can free us all from tyranny. Apple updated the commercial for its January 2004 MacWorld Expo, adding an iPod and earbuds to the outfit of the sledgehammer-wielding athlete.

The following month, a Tunisian lawyer and human rights activist named Riadh Guerfali, known publicly before his country’s 2011 revolution only by his pseudonym, Astrubal, uploaded a mash-up of the ad onto the video-sharing platform Dailymotion. He replaced the on-screen Big Brother with video of President Zine El Abidine Ben Ali. After the athlete sledgehammers the screen, the screen goes white and

the video cuts to a Tunisian girl with her eyes shut. She opens her eyes, as if waking from a bad dream. The video ends.

Guerfali's video was part of a broader digital activism campaign that he and a group of Tunisian activists launched in 2002, before YouTube was invented and before Facebook and Twitter were even twinkles in their creators' eyes. Their strategy was to counter the constant stream of government propaganda with clever antigovernment "propaganda" of their own.

In response, the Tunisian government developed the Arab world's most sophisticated censorship regime. But censorship was not the only way in which the Tunisian people's digital rights were regularly and systematically violated. Digital surveillance in Tunisia was even more pervasive than in Egypt. Progovernment hackers attacked dissident websites with aggressive "denial of service attacks" and took them offline. Government-controlled companies that provide Internet service to offices and homes used "deep packet inspection" technologies to track and filter everything passing through their networks. Government-employed geeks hacked into activists' computers and stole information, intercepted and even altered people's e-mails, and took over activists' Facebook accounts by intercepting their passwords.

After the revolution, several former dissidents and government critics were brought into Tunisia's transitional cabinet—including the dissident blogger Slim Amamou, who had spent the final weeks of Ben Ali's reign in jail for his digital activism. But arguments quickly arose over exactly how free Tunisia's information networks ought to be. Less than a week after the new post-Ben Ali government had formed, Tunisian State Secretary Sami Zaoui announced that the government would continue blocking websites deemed to be "against decency, contain violent elements or incite to hate." In response to fierce backlash by the Tunisian free-speech movement, he retorted on Twitter, "Wrong! Even the countries that are most evolved when it comes to freedom block terrorist sites." Five months later, the government blocked a number of Facebook pages and groups, citing concerns over inflammatory and offensive speech. Amamou resigned in frustration. Guerfali commented philo-

sophically, "Before things were simple: you had the good guys on one side, and the bad guys on the other. Today, things are more subtle."

George Orwell published *1984* at the dawn of the Cold War, as a warning about the totalitarian possibilities of a modern industrialized state that combines centralized power, utopian ideology, and electronic media. The struggle for freedom in the Internet age is shaping up to be very different from the ideological struggles of the twentieth century. Today's struggle is not a clear-cut contest of democracy versus dictatorship, communism versus capitalism, or one ideology over another. Human society has acquired a digital dimension with new, cross-cutting power relationships. The Internet is a politically contested space, featuring new and unstable power relationships among governments, citizens, and companies. Today's battles over freedom and control are raging simultaneously across democracies *and* dictatorships; across economic, ideological, and cultural lines.

Internet platforms and services, made commonplace by companies such as Apple, Google, Facebook, and Twitter, along with a range of mobile, networking, and telecommunications services, have empowered citizens. They have empowered us to challenge government, both our own as well as other governments whose actions affect us. But the Internet also empowers governments themselves—or at least the growing number whose police, military, and security forces understand how the Internet works and who have learned the value of employing computer-science graduates. *All* governments, from dictatorships to democracies, are learning quickly how to use technology to defend their interests.

Apple's dramatic 1984 Super Bowl ad notwithstanding, in reality the interests and loyalties of corporations are divided. On the one hand are the customers and users—also citizens of polities—whose trust is required for long-term business success, and who themselves hold a range of often-conflicting beliefs and values. On the other hand are governments, whose approval and regulatory support is critical if the corporations are to run profitable businesses or gain access to lucrative markets, and who are often important customers themselves. In an ideal world, the government would serve citizens' interests and ensure that their

rights are protected. In the real world, we are not so naive as to assume this is the case, certainly not in authoritarian dictatorships and, depending on one's political viewpoint, not always in democracies either.

The problem is that our ability to organize and speak out is shaped—often quite subtly—by the Internet service providers, e-mail services, mobile devices, and social networking services. If our communications and access to information are manipulated in ways we are not aware of, and if these companies' relationships with government are opaque, our ability to understand how power is being exercised over us, and our ability to hold that power to account, will be eroded in a more subtle and insidious manner than Orwell ever imagined.

In the Internet age, the greatest long-term threat to a genuinely citizen-centric society—a world in which technology and government serve citizens instead of the other way around—looks less like Orwell's *1984*, and more like Aldous Huxley's *Brave New World*: a world in which our desire for security, entertainment, and material comfort is manipulated to the point that we all voluntarily and eagerly submit to subjugation. If we are to avoid this dystopian fate, political innovation will have to catch up with technological innovation.

CORPORATE SUPERPOWERS

In an April 2011 town hall meeting at Facebook's Palo Alto headquarters, President Barack Obama waxed enthusiastic about the political power of social networking:

Historically, part of what makes for a healthy democracy, what is good politics, is when you've got citizens who are informed, who are engaged. And what Facebook allows us to do is make sure this isn't just a one-way conversation; makes sure that not only am I speaking to you but you're also speaking back and we're in a conversation, we're in a dialogue. So I love doing town hall meetings. This format and this company I think is an ideal means for us to be able to carry on this conversation.

For any citizen who cares about politics, this sounds very exciting. But when we step back and think about it more broadly, it is unclear what the president's growing reliance on Facebook for political campaigning and policy advocacy ultimately means for American democracy. Will the result be a net plus for improving American democracy and making government more accountable? Or will a codependency between politicians and social networking platforms result in ever more subtle manipulation of the public discourse?

Meanwhile, Facebook, like any large organization with global interests, has been working hard to win friends and influence people in Washington and other world capitals, to maximize its profit-making potential. In 2010 and 2011, the company beefed up its Washington-based policy team, not only to lobby against regulations that the company believes hamper its interests, but also to help politicians integrate Facebook as a key tool for election campaigns as well as for constituent communications. In May 2011, the company also announced that it would dispatch emissaries to major world capitals to "promote the uses of Facebook with policymakers and influencers in both electoral and governing bodies," and "monitor legislation and regulatory matters." After all, with 600 million users by mid-2011, the social network has more users than most countries have citizens. Facebook, however, was not the first company to create a quasi-diplomatic corps. Since 2005, Google has been hiring executives with government and diplomatic experience for positions described internally as "foreign minister" and "ambassador."

The new digital superpowers have begun to clash with conventional nation-states. A classic example was Google's clash with the Chinese government. In March 2010, Google stopped censoring its Chinese search engine, Google.cn, and moved it out of mainland China in response to aggressive and sustained attacks launched from Chinese computer servers on Google's Gmail service a few months before. The Chinese government denied knowledge of or connection with the attacks, denials that security experts and Western diplomats found difficult to believe given the attacks' military-grade sophistication. Plus Gmail also happened to be the e-mail service of choice for Chinese dissidents and activists, in addition to being

popular among businesspeople, computer programmers, academics, and students. An editorial in China's state-run *People's Daily* responded to Google's defiance of censorship and withdrawal by calling the company "a tool of the US to implement its Internet hegemony." If Google was not going to obey censorship orders and respect Chinese law, officials said, then good riddance. Yet in the end, Google was not fully banned from China. It retained its license to keep a business presence in China and continued some activities not related to search: Android mobile phone operating system development and support, advertising sales, plus research and development for future products.

The reason has to do with Google's own Chinese constituency: people who need access to at least some of Google's products and services to do their jobs and build their own innovative businesses. In the first three months of 2010, when Google's fate in China remained uncertain, people in Beijing and Shanghai laid flowers outside Google offices, as if to commemorate the death of a relative. Many people commented in chat rooms and on social networks, and even told reporters, that they did not know how they could do their jobs effectively, or keep up on the latest research in science and technology around the world without access to Google. Heavy reliance on Google services among foreign businesspeople and investors in China, plus Google's appeal to a certain cohort of educated, professional, urban Chinese—and particularly among China's own technical and business community—was believed to be a big reason the Chinese government did not order a block on all Google services (including Gmail, Google Docs, Google Scholar, and Google Reader) that year.

Some influential Chinese businesspeople argued that an outright ban on Google was simply not in the interest of Chinese industry. Though most expressed this view in private, one prominent member of the business community, Edward Tian, founding CEO of China Netcom, China's first broadband company, spoke out in a public conference, asking, "When we make this sort of company such a big rival, are we not also rejecting these technologies?" Banishing one of the world's most innovative companies from China, he warned, could hurt Chinese com-

panies' ability to innovate and compete in the global marketplace. As the Chinese blogger Michael Anti commented to me wryly at the time, "Google is much more popular in China than the USA." Almost no Chinese citizens consider themselves stakeholders or constituents of the United States. But Google has many Chinese constituents. They are, in effect, digital residents of Googledom: a global community of people who rely on certain Google services.

In late 2010, Google CEO Eric Schmidt and Jared Cohen (who had just left the State Department policy planning staff in the summer of 2010 to run Google's new policy think tank) published an article in *Foreign Affairs* outlining their geopolitical vision for a digitally networked world. "Democratic governments," they wrote, "have an obligation to join together while also respecting the power of the private and nonprofit sectors to bring about change." They warned against overregulation of Internet companies, lest their greatest value to citizens be stifled.

Google and Facebook are just two of the many companies whose products and services have created a new, globally networked public sphere that is largely shaped, built, owned, and operated by the private sector. Digital platforms, services, and devices now mediate human relationships of all kinds, including the relationship between citizens and government. Struggles to control and shape this sphere are intensifying around the world. These struggles will only escalate as the stakes continue to rise.

There is no question that the Internet would not be what it is today, and could not fulfill its potential as an empowering force for the disaffected, ignored, and oppressed, without a vibrant and innovative private business sector. Successful businesses need regulatory and legal environments that allow private citizens to form companies, borrow money or obtain investment, and protect their rights to property and inventions—both physical and virtual. It was no accident that Microsoft, Apple, Google, and Amazon were spawned by entrepreneurs in the United States and not in other countries with more constrained regulatory, entrepreneurial, and political environments.

Many people around the world are concerned, however, that Internet and telecommunications companies have gained far too much power

over citizens' lives, in ways that are insufficiently transparent or accountable to the public interest. In just one of many examples, German and Korean citizens were particularly outraged by what they perceived to be an unjustified invasion of their privacy by Google Street View, a global service that enables people to zero in on a map to see in minute detail what any given street or neighborhood looks like. In April 2011, researchers exposed that Apple iPhones were logging and storing detailed information about users' movements, unbeknownst to most iPhone users. (Apple later fixed what it described as a "bug" in the phone's operating software.)

Companies argue that collecting a wide array of personal data is necessary to serve people better, in ways most people have shown that they want. Critics argue that companies have gone far beyond what most citizens *actually* want—when they have a chance to understand what is really going on. In his book *The Filter Bubble*, Eli Pariser warns that search engines and social networks manipulate what we find and who we interact with on the Web in a way that maximizes our value to advertisers but that is likely to minimize the chances that we will be exposed to a sufficiently diverse range of news and views that we need as citizens to make informed political and economic choices. In *The Googlization of Everything*, Siva Vaidhyanathan warns that Google in particular represents a new ideology that he calls "techno-fundamentalism," which encourages a dangerously "blind faith in technology" on the part of people who use Google services. Such faith, he argues, blinds us to what companies might be doing differently, how their internal decisions affect our lives in ways we have never thought about, and whether our excitement with new technologies lulls us into accepting risks that we do not see or understand.

The geopolitical power of corporations has been growing for decades and is certainly not limited to Internet-related companies. As Harvard's Joseph Nye points out in *The Future of Power*, when a corporate giant like IBM derives two-thirds of its revenue from outside its home US base, with only one-quarter of its workforce living in the United States, the conventional power politics of nation-states is disrupted by the

emerging power of the private sector. Approximately half of the world's one hundred largest economic entities are now corporations. If Walmart were a country, it would be the world's twenty-fifth-largest economy in terms of GDP, ahead of countries such as Norway, Venezuela, and the United Arab Emirates.

Other kinds of transnational organizations are also challenging the power of nation-states. International institutions such as the United Nations, the World Bank, and the International Monetary Fund, set up at the end of the Second World War, use the nation-state as their organizing principle, while the world's power dynamics increasingly are driven by a much more diffuse set of actors. Newer organizations like the World Economic Forum, along with so-called multi-stakeholder corporate responsibility initiatives, create spaces where states, nongovernmental organizations (NGOs), and corporations can meet if not as equals, then at least as joint actors based on the premise that solutions to global challenges are beyond the legitimacy and capacity of any one sector to succeed.

It is now normal for the world's most powerful governments to consult with multinational corporations to shape a range of financial, trade, and foreign policy objectives. Not only are the world's most powerful democracies prodded and shamed by international NGOs like Human Rights Watch, Global Witness, Oxfam, and Greenpeace, but governments also increasingly find themselves needing to coordinate with—and even answer to—these and many other organizations in addressing a range of human rights and developmental issues. Companies and NGOs now show up in force to lobby their interests and causes at UN meetings on problems ranging from climate change to the new and thorny question of Internet governance.

Internet-related companies are even more powerful because not only do they create and sell products, but they also provide and shape the digital spaces upon which citizens increasingly depend. Governments of all kinds seek to control them precisely because of this power. Amid such dramatic changes in the power dynamic, it is important to remember the original purpose of democratic government and politics: to ensure that citizens' interests are served and that their rights are protected.

LEGITIMACY

The idea of the nation-state as the main organizing unit for politics and geopolitics, and the further notion that nation-state governance should be grounded in "consent of the governed," are both relatively new ideas that did not spread on a truly global scale until the late twentieth century. Modern concepts of sovereignty and legitimacy first germinated eight hundred years ago when a critical mass of English nobility decided that the unconstrained "divine right of kings" no longer served their interests, and realized that they had the economic and military power to do something about the situation. In 1215 at a field called Runnymede, the English nobility, fed up with arbitrary jailings, confiscations of property, and what they felt were other unreasonable violations of their rights, forced King John to sign a document called the Magna Carta. This "great charter" recognized that even kings must be bound by law and unleashed a powerful set of ideas about legal rights and political sovereignty.

The Magna Carta was the first attempt in the Western world since the ancient Greeks to enshrine the idea that a sovereign's legitimacy does not derive solely from divine right and brute force; even the king is subject to the law. Though the barons were hardly populists, let alone revolutionaries—their goal was to protect the interests of an elite ruling class—the Magna Carta nonetheless laid the groundwork for the concept of the modern nation-state, based on the rule of law over men.

It would take four more centuries for the sovereignty of the modern nation-state to be formalized in Europe by the 1648 Treaty of Westphalia. Political philosophers from Hobbes to Locke to Rousseau expanded and broadened the idea of "consent of the governed." In 1647 during the English civil war, a scrappy group of commoners calling themselves the Levellers issued a declaration of rights, including assertions that all citizens have the right to liberty of conscience and religion; that all laws must respect all persons equally, regardless of wealth, nobility, or lack thereof; and that Parliament must pass no law "evidently destructive of the safety or wellbeing of the people."

The Levellers debated their allies against King Charles I in Putney Church on the banks of the Thames: a physical commons for political discourse in which sovereignty and consent were freely debated in the most radical terms yet in English history. Even though they failed, their ideas eventually inspired the American Declaration of Independence and the Bill of Rights, and became the building blocks of the United Kingdom's modern parliamentary system. The Magna Carta is the antecedent and the Levellers are the ancestors of democracy movements and human rights struggles around the world. They are also the progenitors of modern struggles for civil liberties in today's democracies, as citizens never stop fighting to bring their societies closer to their founding ideals.

The Internet holds immense potential to help citizens improve democratic governance where it already exists, and has proven to be an effective tool in the hands of activists in exposing injustice and even overthrowing dictators. It offers a global platform for public discourse on matters of sovereignty and consent—yet those ideals are contested and even imperiled within the digital commons.

In his 2009 book, *Communication Power*, Internet scholar Manuel Castells recounts the numerous victories of popular movements and Internet-powered grassroots campaigns around the world over the past decade, describing how "insurgent communities" have managed to "re-program" national politics in many countries. Yet he ends with a warning: digitally empowered citizens may have won important victories, but these victories are not necessarily permanent "because the powerholders in the network society" will do everything possible to "enclose free communication in commercialized and policed networks."

We would do well to heed Castells's warning. As the Internet grows ever more intertwined with our lives, citizens' dependence on it for achieving and sustaining democracy also grows. In our dependence, we have a problem: we understand how power works in the physical world, but we do not yet have a clear understanding of how power works in the digital realm.

The point of democracy is that power, when unchecked, will be abused by any person or group of people with the opportunity to wield

it. More than three hundred years since the Treaty of Westphalia and over two hundred since the world's first democracy was established, we have a reasonable understanding of how nation-states wield power and how state power can be constrained by constitutions, elections, laws, and international treaties.

We lack a similar understanding of how various kinds of transnational digital platforms and the organizations that build them derive and wield their power; to whom, if anyone, they are accountable; and how their power can best be constrained in a way that does minimal harm and maximum good. Many Internet and telecommunications companies have created powerful platforms for citizens to challenge governments. Yet there is no clear model for constraining these companies' power in a way that does not also diminish their value as globally interconnected spaces.

Amid all of our excitement over new technologies, our default assumption as citizens must be that governments, powerful corporations seeking market dominance, and various other interest groups will use digital networks to obtain and maintain power whenever the opportunity presents itself. If existing institutions and mechanisms are inadequate to constrain the abuse of power across globally interconnected digital networks, political innovation must catch up to technological innovation.

Democracy was never advanced by people asking politely. Building and preserving democracy in the physical world remains a constant struggle. Conceiving and implementing a governance structure for a globally interconnected digital world that constrains the abuse of both government and corporate power and protects individual rights—based on the notion of consent of the networked—is not going to be any easier.

A first step in that direction is to acknowledge, protect, and nurture a powerful counterweight to government and corporate power: the digital commons.

CHAPTER 2

Rise of the Digital Commons

One Saturday morning in September 2007, roughly one hundred people—most of them well under thirty years old—trickled into an auditorium at Tsinghua University, China's most prestigious school of science and engineering, for a one-day gathering called WordCamp. Many had come specifically to meet Matt Mullenweg, a twenty-four-year-old college dropout from Texas.

In 2003 Mullenweg launched an open-source blog publishing software program called WordPress. Unlike commercial blogging software offered by companies, WordPress welcomed anybody with software programming skills to modify its software code. In that way, people could shape WordPress to fit their own specific needs, which the original creators were unable to anticipate. The free software quickly formed a global community of developers who expanded its features and functionality, so that it could be used for a range of online publishing purposes. It has been translated into a range of languages. It powers a vast range of sites from Global Voices to the Kenyan citizen media website Ushahidi, to several Arabic blogging community websites. It also powers the blogs of some of China's most cutting-edge bloggers.

One of the WordPress fans who clamored for a photo with Mullenweg at Beijing WordCamp was Zhou Shuguang, a twenty-eight-year-old vegetable seller turned blogger who writes under the pen name Zola. This "citizen journalist" has traveled the country writing about hot topics on the Chinese Internet. In 2006 he catapulted to fame as the

"nailhouse blogger" whose on-site reports of a dramatic standoff between a Chongqing couple and local property developers helped break down a national media ban on the incident. In 2007 he was detained and escorted back to his home in Changsha after attempting to cover protests in the Northeast. In 2008 he went to the Sichuan earthquake zone to document the situation, then to Weng'an in Guizhou province, where there had been riots related to seething anger over abuse of power by local authorities and their relatives. He planned to go to Beijing for the Olympics, but police ordered him to stay home. As soon as the Olympics were over, he went to meet Mullenweg, his guru.

Zola runs his blog on WordPress; he has no other good publishing option. Most of China's 200 million bloggers use services hosted by Chinese companies. In exchange for the convenience of not having to worry about technical setup, these services control what their users can publish and are required by the government to censor heavily for politically sensitive content. Zola tried blogging on several of these platforms, but his posts kept getting taken down. Then he bought server space from a Chinese domestic web-hosting company and set up his own blog using WordPress, hoping to be free of control. But several Chinese web-hosting companies—also required to police the websites they host for politically sensitive content—shut down his site. Finally Zola had no choice but to find space on an overseas web host and to set up his WordPress blog there. Zola has little money, so he relied on free hosting from people interested in helping him. Since WordPress software is also free, Zola was able to customize it, with help from other members of the global WordPress developer community, adding special technical features that would enable his readers to connect to his site securely, allowing people to leave comments anonymously on his site.

WordPress, and the community of bloggers who use it and improve upon it, is just one small part of a much larger phenomenon known as the "sharing economy" or the "digital commons": an important reason the Internet is so revolutionary and disruptive. A robust digital commons is vital to ensure that the power of citizens on the Internet is not ultimately overcome by the power of corporations and governments.

In the early 1800s, when the United States was still a novel political experiment, Alexis de Tocqueville observed in his classic book *Democracy in America* that the key to functional democracy was a vibrant "civil society." He described the importance of active involvement by citizens in community life: people from all social strata and professions taking personal responsibility for the safety and well-being of their communities, pushing back against perceived infringements of their rights, and sharing ideas and forming associations to solve problems and improve life for everybody.

The digital commons is the virtual equivalent of Tocqueville's civil society, through which citizens can mobilize to express their interests and protect their rights. Ideally, the digital commons—comprising primarily a collection of technical standards and free and open-source software programs, plus a range of digital media creations—can exist in a positive and symbiotic relationship with both government and the private sector. But when governments or corporations abuse their power, the commons can act as a counterweight and support network through which citizens can carve out the necessary spaces to speak and organize, and thus defend their rights and interests.

In his book *The Wealth of Networks*, Harvard law professor Yochai Benkler describes how the Internet is both the product and the incubator of "commons-based information production, of individuals and loose associations producing information in nonproprietary forms." Without their efforts, neither the Internet nor the World Wide Web—with their tremendous commercial value and political power—would exist. The digital commons is a vast and growing universe of engineering inventions, software, and digital media content, created by people who have chosen to share their creations freely, because the material barriers to and costs of organizing have dropped dramatically.

THE TECHNICAL COMMONS

Millions of coders and engineers—some working for companies to make products for sale, some collaborating in communities to create

open standards and free software—have collectively built a globally networked resource used by more than two billion people. The technical standards upon which the Internet and the World Wide Web depend are at the core of the digital commons: they are not copyrighted or trademarked. They are free and open to all. The Internet's inherent value and power come from the fact that it is globally interoperable and decentralized, so that everybody can add to the network and create products, services, and platforms on top of it without having to obtain permission or license, or some kind of access code, from anybody in particular. Some people choose to make businesses from their creations, others choose to share them freely, benefiting in nonmonetary ways from doing so.

The technical protocols that enable different kinds of computers and software to communicate with one another across networks are called TCP/IP (Transmission-Control Protocol/Internet Protocol). These protocols were developed by engineers working across a variety of research labs and companies. They agreed to share the protocols openly to facilitate the Internet's broader adoption and use. Imagine what would have happened if they had instead slapped a patent on their invention and tried to charge licensing fees to anybody who wanted to incorporate TCP/IP standards into their computers, software, or networking devices. The Internet would not be what it is today if those engineers had been unable or unwilling to share TCP/IP freely with the world as part of the digital commons.

The World Wide Web, invented two decades after the Internet, similarly owes its existence to the digital commons. What we call "the web" is an interlinked universe of websites accessed through web browsers such as Internet Explorer, Safari, and Firefox. All websites, no matter where they are created or what kind of computer system is used to host them, are readable from anywhere thanks to a common computer language called the hypertext mark-up language (HTML). The web is how most people on the planet today use the Internet. We can thank the Englishman Sir Tim Berners-Lee (eventually knighted for his invention), who in 1990 while at the particle physics lab at the European Organi-

zation for Nuclear Research in Switzerland wrote a simple computer program called the WorldWideWeb to make it easier for researchers in his lab to locate and share each other's data. Sir Berners-Lee did not try to patent or charge for the use of his HTML language and the web-addressing system he created; instead he released them into the public domain. The Web would not be truly worldwide had he sought to license the use of the language that enables people to create websites.

Even though the digital commons is based on protocols and technologies that were developed noncommercially, Internet companies like Google have had a symbiotic and overlapping relationship with the digital commons from the beginning. None of these businesses would be what they are today if it hadn't been for the work that network engineers and computer scientists contributed to the commons. For this reason, most large Internet companies—from Cisco, AT&T, and Intel to Microsoft, Google, and Facebook—support and participate in the work of open standards organizations (such as the Internet Engineering Task Force, or IETF, and the World Wide Web Consortium, or W3C) and the coordinating bodies that maintain the global addressing and domain name system (like the Internet Corporation for Assigned Names and Numbers, or ICANN, and regional Internet registries). These organizations maintain, update, and add to the technical standards necessary to keep the Internet running on increasingly sophisticated devices used by almost two billion people around the planet. Governments do not run any of these organizations.

Some countries—China, Iran, and Brazil, to name a few—have lobbied for the United Nations to take over these organizations and coordinating bodies. Other countries, including the United States, are opposed. So are human rights groups and most major Western Internet companies; Google has taken a particularly public stand on this issue. Most Internet users around the world are unaware of this increasingly high-stakes fight over the future of Internet governance, a geopolitical battle with implications for the future political freedoms of all citizens.

The free-software and open-source software communities are also key to the expansion and growth of the digital commons, upon which a

great deal of both commercial and noncommercial activity now depends. In 1989, the computer scientist Richard Stallman got the ball rolling when he created the General Public License (GPL), which authorizes anybody to use a GPL-licensed software program as long as any copies or derivatives are also made available on the same terms. This license enabled software programmers to contribute computer code with the express purpose of sharing it with others, who can in turn build and improve on it, on the condition that the modifications and improvements remain part of the commons.

GPL software licensing was brought into the global prime time by Finnish computer scientist Linus Torvalds, who created the "kernel" of the Linux computer operating system, which programmers all over the world have worked to build upon and improve. In 2000, IBM adopted Linux as the centerpiece of its service and consulting business. By 2008, 60 percent of the world's computer servers ran on Linux, with a minority 40 percent using Microsoft's proprietary Windows platform. Open-source web server software called Apache runs more web servers in the world than any other, beating out all commercial alternatives. Open-source website design and management software like Drupal and WordPress—developed by a global community of programmers—run the websites of millions of small businesses as well as millions more blogs and nonprofit websites. Human rights groups, small news organizations, community media groups, and activists around the world are heavy users of open-source software. Many of the digital activists who helped bring down the governments of Egypt and Tunisia were heavy users of—and in some cases contributors to—open-source software.

Open-source software is not inherently antibusiness. Some open-source projects and communities work separately or even in direct competition with companies, but many work in a symbiotic relationship with for-profit businesses. Google heavily uses and contributes to the digital commons, and so does Facebook. The Android mobile operating system developed by Google runs on Linux, and its openness is one of the key reasons Android has quickly become a key driver of the global smart-phone market. According to the Linux Foundation's 2010 annual

report, since 2005 around 6,100 individual developers and six hundred companies have contributed to the Linux kernel.

In December 2010, Reuters News Agency reported that more than 70 percent of contributions made to the Linux code base "are from developers who are getting paid for their Linux development from corporations who hope to benefit from better software in their core business." In a 2009 speech, Jim Zemlin, executive director of the Linux Foundation, pointed out that every Internet user on the planet is a Linux user in some way or another, because there is almost no digital product or service today that does not rely upon or in some way benefit from the open-source operating system.

ACTIVISM

The digital activists who played a key role in bringing down the governments of Tunisia and Egypt did not spring immaculately from Facebook and Twitter. They started building interconnected online and offline movements well before either service was conceived, using a variety of platforms, services, and software—some built by companies, some built by themselves or created noncommercially by others. They were also major contributors to—and beneficiaries of—the digital commons.

Riadh Guerfali and Slim Amamou, plus a number of others including Sami Ben Gharbia, a Tunisian dissident exiled in the Netherlands, started experimenting with online activism back in 2000. Their first project was an online magazine on which they posted articles e-mailed to them by less tech-savvy Tunisian dissidents and activists who were banned from publishing in Tunisia and had no other way to get their information disseminated. In 2004 they used WordPress to create Nawaat.org, a website that later won awards for its role as an information hub for activism during the "jasmine revolution" of late 2010 and 2011.

For the next five years, Nawaat's importance grew as a hub for videos, photos, and articles about the human rights situation in Tunisia, the latest outrages of Ben Ali's regime, information and updates on what was being censored and how, plus tutorials about how to get around

ensorship and evade surveillance. Nawaat's material was published under a Creative Commons (CC) license, a more open form of copyright licensing—inspired by the .GPL open-source software licensing system—which allows content to be shared and copied freely as long as credit is given to the original source. This type of licensing is particularly useful for activists and civic organizations trying to reach wide audiences and whose primary purpose is not financial profit. CC licenses encourage people to copy and republish activist content without worrying about being accused of stealing or pirating content that was, after all, created with the express purpose of being shared and viewed as widely as possible.

As new start-up companies in Silicon Valley and elsewhere spawned new social media tools, the Nawaat team quickly adapted them for activism. Not long after Google launched Google Maps, for example, Sami Ben Gharbia used it to create the Tunisian Prison Map, calling attention in a dramatic and visual way to just how many political prisoners were being held around the country. Though much of Nawaat's content is republished on YouTube, Flickr, and Facebook and is promoted heavily on Twitter, the activists learned early how important it would be to keep all of their content archived on their own platform, over which they have complete control. At one point Nawaat's YouTube channel was frozen by company administrators because somebody—nobody knows who—filed a complaint through YouTube's internal abuse-reporting system that some of the channel's content violated the company's terms of service. Similar complaints were frequently filed against the accounts of Nawaat team members on Facebook, because its terms of service require that people use their real names on their account—something that was too risky for most Tunisian dissidents, who preferred to use pseudonyms in hopes of not becoming another data point on the Tunisian Prison Map.

Over the years, Tunisian activists developed close ties with bloggers and activists around the Arabic-speaking world, and particularly bloggers from Egypt, which happened to be home to a highly educated, early-adopting techie community. By 2004, Egyptian bloggers were collecting and disseminating information about arrested activists, as well as

shocking acts of torture by the Mubarak regime's police forces. A number of these bloggers were arrested in connection with offline street protests as well as online writings. When arrests took place, other bloggers used all digital platforms available to raise public awareness about what had happened to them and to circulate information about their arrests and activities throughout the Arabic-language blogosphere.

One of many activists who spent time in jail during those early days of online activism was Alaa Abd El-Fattah, who in 2004 with his wife, Manal, also a blogger, used the open-source publishing software Drupal to launch a website aggregating the posts of Egypt's political bloggers. The Egyptian Blogs Aggregator helped to build a community of people who then—like the Tunisians—adopted whatever social networking and web tools best served their purposes. By 2006 Facebook had gained a critical mass among young Egyptian Internet users. A group of young activists found it to be particularly useful in organizing street protests, as well as to call attention to the arrests of their friends. The rest is history. In 2010 after the death of a young man named Khaled Said at the hands of Egyptian police, Google executive Wael Ghonim, using a false identity, created the Facebook page "We are Khaled Said," which became a hub for organizing antitorture protests in 2010 and organized the first protest in Tahrir Square on January 25, 2011, after which events snowballed.

Before the Arab Spring of 2011, during which protest movements organized in part with the help of the Internet successfully toppled the leaders of Tunisia and Egypt and inspired revolts around the region, Tunisian and Egyptian bloggers played leading roles in organizing two pan-Arab blogger conferences. The Arab Techies Collective, formed in 2008, brought together a more technical group of software developers and web designers from around the region, who collaborated on open-source software development projects. They worked together to modify, improve, and customize open-source software that they found particularly useful for Arabic-language activism, translating software interfaces as well as manuals into Arabic. The Arab techies also developed ties with developer communities in the United States, Europe, and Asia. These online and offline ties were put to good use as tensions began to

rise in Tunisia and then in Egypt. As websites around the region were blocked and hacked by governments seeking to thwart their movement, activists already knew whom to contact in a global community of developers who work on open-source anticensorship and anonymization software. An international community of "hacktivists" quickly reached out to help.

Given their preexisting ties with activist hackers around the world, it was not surprising that the Tunisian activists running Nawaat were able to get ahold of WikiLeaks' trove of US diplomatic cables pertaining to the Ben Ali regime. The revelations posted on the website they created, Tunileaks, confirmed to the Tunisian public that US diplomats viewed the Ben Ali regime as corrupt and increasingly dysfunctional, despite not saying so publicly due to Ben Ali's perceived helpfulness in the war on terror. The information published by Nawaat and Tunileaks is believed by diplomats, human rights groups, and journalists who have since gone back and analyzed the Tunisian revolution to have contributed in no small part to Tunisians' rejection of the Ben Ali regime. This explanation rings true given the timing of the information's release, as street protests mounted in the wake of the self-immolation of a desperate vegetable seller in the town of Sidi Bouzid.

The emergence of the Arab digital commons and its natural relationship with the broader global commons is a textbook example of what Clay Shirky, a technology and social theorist at New York University, has described in two influential books about how people use and contribute to the commons. The Internet, he argues, makes it easier than ever for the civic-minded to rally around a cause and to push for change. Wikipedia, the all-volunteer, peer-produced online encyclopedia, was perhaps one of the earliest and most dramatic examples of this phenomenon. Blogging, tweeting, podcasting, and taking pictures and videos and uploading them to Flickr and YouTube can all be done at near-zero financial cost.

Such "social production" is not exclusive to any side of the political spectrum or to a particular set of values. Viral homemade videos on YouTube helped mobilize young people to volunteer on the campaign

trail and vote for Barack Obama in 2008. Similar tools and activities were key to the Tea Party-led Republican takeover of the US House of Representatives in 2010. WikiLeaks, the whistle-blowing website most famous for its controversial release of leaked US diplomatic cables, is also part of the digital commons.

BALANCE OF POWER

Though the digital commons played a vital part in facilitating the Arab Spring, it is less clear how it will contribute to Arab democracy. What is clear, however, is that software code and technical infrastructure have an important role in mediating the relationships between citizens of these countries and their new governments—alongside laws, constitutions, institutions, and political processes.

As Harvard law professor Lawrence Lessig explained more than a decade ago in his seminal book, *Code and Other Laws of Cyberspace*, software code and technical standards are for all practical purposes a new form of law, because just like laws, they shape what people can and cannot do. The implications are massive. In the pre-Internet era, government—which in democracies at least is expected to reflect "consent of the governed" and to be held accountable to the public interest—had the primary responsibility for developing legal codes governing what people did in the physical world, backed up by the authority and force necessary to enforce meaningful levels of compliance. In the Internet age, a whole new sphere of *de facto* lawmaking has emerged in the guise of software code and technical standards that channel and constrain what people do with their technology. In this way, the power to shape how citizens can organize, access and disseminate information, and express their own ideas and opinions has expanded dramatically to anybody who knows how to write software code, create Internet and telecommunications hardware, and build interoperable networks. Right now this power is wielded primarily by a combination of people who are either working in service of companies or contributing to the commons in some fashion.

People who contribute to the digital commons and who act as its stewards, architects, and defenders are engaging in a form of citizenship for the Internet. Some now call this "netizenship." David Bollier, whose book *Viral Spiral* documents the rise of the digital commons in the United States, argues that the people who build and contribute to it—the "commoners"—have "invented a new sort of democratic polity." Many American and European technologists assume in their writings that the emergent digital commons is inherently more democratic than any existing parliamentary democracy, because governments and laws tend to lag hopelessly behind technological change. But is it logical to assume that a new digital civil society, whose vanguard is led by computer programmers, tech-savvy early adopters belonging to a range of groups, hackers, and bloggers with a range of political and economic agendas, will necessarily serve the interests and respect the rights of all people who use the Internet across the globe? Who has the right to impose their ideas of right and wrong in shaping the network's future?

Despite the optimism of Bollier and many Western technologists, unless human nature undergoes some sort of fundamental transformation, it seems inconceivable that the world's "netizens" will naturally act, in aggregate, in a way that serves the common good and respects the rights of all vulnerable minorities and people with peaceful but unpopular views. A system is needed to reward good behavior and punish bad behavior as well as general consensus around what constitutes "good" and "bad." Plenty of crime and acts of cyber-warfare are committed through the Internet and with the help of the commons.

Different "netizens" have different political loyalties: there are pro-government bloggers and hackers in China, Iran, Russia and many other countries, proudly ready to attack their government's perceived and imagined enemies. There are jihadist programmers. There are vigilante hacker groups like Anonymous, who launched "denial of service" attacks against businesses that cut their ties with WikiLeaks, and who have been known to attack the websites of other entities whose values its members disapprove of. Though most members of Anonymous view themselves as freedom fighters protesting the unjust power of governments and cor-

porations over people's digital lives, one can make a strong case that their chosen form of protest harms innocent people (i.e., customers and users of the services they are attacking) and is unconstructive when it comes to building a more rational and equitable set of power structures over the long term. They are more like Robin Hood, deliberately committing crimes in response to King John's governance failures, than the Levellers of the English civil war, who fought to change an elitist political structure, or the American revolutionaries who sought to build an alternative system of governance to replace an unjust one.

The need to protect the rights of unpopular minorities, the less tech-savvy, and other innocent people from criminals is one of many good reasons that the need for democratic government—governance based on consent of the governed—will not go away. Doing away with geographically based governance is not a good idea either: citizens remain at core flesh-and-blood people with physical and often very local needs. At the same time, the power of multinational corporations continues to grow, empowering and employing tens of millions while also displacing and exploiting others. It is clear to anybody who pays attention to the news that these two pillars of global society, governments and companies, cannot be counted upon alone—and even less so together—to protect the rights or serve the interests of all the world's people, in either physical space or digital space. The citizen commons—parts of which are very local and regional, and parts of which are very global—is thus a vital counterweight to government and corporate power in cyberspace. The commons provides the space, tools, and community that allow people to build noncommercial, secure, and private spaces that enable dissent, whistle-blowing, and nonmainstream conversations.

Today the existence and importance of the commons is not well recognized, valued, or understood even by many of its contributors and participants. Even in the democracies of North America and Western Europe, creators and defenders of the commons are engaged in pitched battles in legislatures and courts against powerful companies, government agencies, and interest groups who find many aspects of the Internet threatening to their businesses, security protocols, and accustomed

ways of life. The weaker the democracy and the weaker its constitutional and legal protections of citizen rights, the more beleaguered the commons becomes, at citizens' expense.

At the extreme end of this spectrum—that is, the spectrum of governments that have learned to actively manipulate technology rather than simply restrict citizens' access to technology, as old-fashioned authoritarian regimes like Cuba and North Korea currently do—is China. The robust, lively, and rapidly growing Chinese Internet is the product of a strong government plus a robust private sector, combined with the absence of democracy, accountable governance, due process, and meaningful protection of citizen rights. China represents a new, upgraded form of the authoritarian state: it embraces Internet connectivity not merely as essential for a world-class economic and financial power, but also as necessary for modern government. At the same time, China's digital commons is under attack and subject to cynical manipulation by the state, with the direct assistance and collusion of the private sector.

PART TWO

CONTROL 2.0

We will never have a real civil society, a democratic society, unless people take responsibility.

—AI WEIWEI, JANUARY 2009

CHAPTER 3

Networked Authoritarianism

In 2009 in Hubei province, a twenty-one-year-old waitress named Deng Yujiao was working as a manicurist for a business that combined the services of restaurant, spa, and salon. Patrons could wine and dine, then relax with a haircut, manicure, and massage without leaving the building; sexual services were also known to be available. A local Communist Party official, entertaining friends at this multiservice establishment, took a shine to Deng. He demanded sex; she refused. He tried to force her. She fought back with a pedicure knife and somehow ended up killing him.

News of the incident quickly spread online. Deng was hailed as a heroine. A blogger tracked down the local mental hospital where she was being held and posted pictures online. Women wrote passionate postings titled "We are all Deng Yujiao." Despite government efforts to control the news, people were simply too angry—about abuse of power by petty local officials, as well as about the economic circumstances that compel young women to make a living in such sleazy establishments. Realizing that a conviction could spark riots, the authorities eventually dropped the murder charges against her. She was convicted on a lesser charge instead and set free.

In the pre-Internet age, such a person would have disappeared into the prison system or into a mental health ward, unbeknownst to anybody other than a few close friends and relations in Hubei. The Internet enables ordinary Chinese people to speak truth to power and pursue

justice in unprecedented ways. At the same time, Chinese Internet users have a manipulated and distorted view of their own country as well as of the broader world.

I had a telling encounter on a recent visit to Peking University. Once a hotbed of political activism during the 1989 student protests, these days the university keeps students under considerably tighter control. I met a doe-eyed undergraduate dressed in stylish jeans and a fuzzy sweater who wanted to interview me for her student magazine. (I will call her "Mary" to spare her trouble and possible embarrassment.) She asked about my experiences covering China as a CNN correspondent and how the Chinese government handled the Western media. I told her my colleagues and I frequently had been detained by police in the 1990s.

"Really? I didn't know that happened to foreign journalists," she said.

"It still does," I replied. "You know of course that Chinese journalists sometimes go to jail if they push too far with their investigative reporting."

Silence. Mary's large black eyes, framed by tasteful amounts of eyeliner and mascara, widened and began to glisten as she stared at me in shock. "I had no idea," she said softly.

In all modern societies, there are heated disputes over how media and information networks are regulated and managed, and the extent to which systemic biases favor people with power and money over those without power or money. But in China there is no transparency or public accountability when it comes to how information networks are shaped, operated, regulated, and policed. This total opacity, plus government co-optation of the private sector in carrying out political censorship and surveillance, are the key components of what I call China's networked authoritarianism. The key to the system's success is that the regime does not try to control everybody all the time; its controls on political information are nonetheless effective *enough* that most Chinese—including educated elites—are unaware, or have a distorted view, of many issues and events in their own country, let alone in the rest of the world.

In 2005 a PBS documentary crew visited university campuses around Beijing and showed students the iconic 1989 photograph of a man standing in front of a tank. Amazingly (at least to Westerners), most didn't recognize the image at all. Chinese university students' blinkered knowledge and understanding of their own society, past and present, is one of the regime's most deliberate and profound achievements.

The 1989 Tiananmen Square protests were sparked by the death of a reformist leader, Hu Yaobang, but the fire was fueled by the historic Beijing visit of Soviet leader Mikhail Gorbachev soon thereafter. Students hoped that Chinese leaders would follow his policy of glasnost, the Russian word for "openness," which became the catchphrase for a loosening of controls on the Russian press and discussion of political reform. After the bloody June 4 crackdown, Deng Xiaoping quashed all hopes that China would follow Gorbachev's lead. Instead Deng focused aggressively and exclusively on the Chinese version of perestroika, or "restructuring": accelerating the economic reforms that have made China the world's second-largest economy today and a rising global power. Deng was betting that most Chinese people would agree that the trade-off between economic prosperity and political liberty was worthwhile—or at least enough of China's elites would believe so and maintain their allegiance to the Communist Party as the guarantor of prosperity and stability.

Deng's efforts have nevertheless given way to a limited sort of cyber-glasnost: people use the Internet to address injustice at the local and personal level, expanding the public discourse and enabling people to speak out on a greater range of issues, while at the same time no meaningful changes have been made to the political system. People who cross the government's political red lines find themselves with no better legal protection than they had twenty years ago. These people include 2010 Nobel Peace Prize winner Liu Xiaobo, who was arrested in late 2008 and sentenced in 2009 to ten years in jail for state subversion for writing the prodemocracy treatise Charter 08. In early 2011 the artist and political activist Ai Weiwei—internationally famous for his unorthodox art installations as well as his outspoken views on corruption and

political reform—was detained and investigated for tax fraud, although it was clear that the real reason for his detention was that he repeatedly linked cases of local corruption and malfeasance with the need for broad democratic reforms.

According to the Dui Hua Foundation, a China-focused human rights research and advocacy organization, in 2008 (the year of the Beijing Olympics) the number of people sentenced for “endangering state security”—the most common charge used in cases of political, religious, or ethnic dissent—more than doubled for the second time in three years. Since then, political arrests have remained substantially higher than in the 1990s, when few Chinese people had Internet access. Thanks to censorship, the average person rarely encounters information about these types of arrests.

A networked authoritarian regime benefits from the lively online discussion of many social issues and even policy problems. The government follows online chatter, which alerts officials to potential unrest, better enabling authorities to address issues and problems before they get out of control. Sometimes people are successful in using the Internet to call attention to social injustice, as in Deng Yujiao’s case. Citizens even manage to use cyber-vigilantism—popularly known as the “human flesh search engine”—to bring about the resignation of corrupt officials. Sometimes laws or regulations are even changed as the result of concerned citizens’ online campaigning. As a result, China’s 500 million Internet users feel more free and are less fearful of their government than in the past. The communications revolution has transformed China in many ways, but the Communist Party has thus far succeeded—against all odds and expectations—in controlling it to remain in power.

HOW CHINA’S CENSORSHIP WORKS

In fall 2009, I sat in a large auditorium festooned with red banners and watched as Robin Li, CEO of Baidu, China’s dominant search engine, paraded onstage with executives from nineteen other companies to re-

ceive the China Internet Self-Discipline Award. Officials from the quasi-governmental Internet Society of China praised them for fostering “harmonious and healthy Internet development.” In the Chinese regulatory context, “healthy” is a euphemism for “porn-free” and “crime-free.” “Harmonious” implies prevention of activity that would provoke social or political disharmony.

China’s censorship system is complex and multilayered. The outer layer is generally known as the “great firewall” of China, through which hundreds of thousands of websites are blocked from view on the Chinese Internet. What this system means in practice is that when one goes online from an ordinary commercial Internet connection inside China and tries to visit a website such as <http://hrw.org>, the website belonging to Human Rights Watch, the web browser shows an error message saying, “This page cannot be found.” This blocking is easily accomplished because the global Internet connects to the Chinese Internet through only eight “gateways,” which are easily “filtered.” At each gateway, as well as among all the different Internet service providers within China, Internet routers—the devices that move the data back and forth between different computer networks—are all configured to block long lists of website addresses and politically sensitive keywords.

These blocks can be circumvented by people who know how to use anticensorship software tools. It is impossible to conduct accurate usage surveys, but it is believed likely that hundreds of thousands of Chinese Internet users deploy these tools to access Twitter and Facebook every day. Yet researchers estimate that out of China’s 500 million Internet users, only about 1 percent or so (a number somewhere in the single-digit millions—still a large number of people but not enough percentage-wise to shape majority public opinion) use these tools to get around censorship, either because most do not know how or because they lack sufficient interest in—or awareness of—what exists on the other side of the “great firewall.”

Fortunately for the government, there are plenty of social networking platforms and other delightfully entertaining and useful services on the Chinese Internet to keep people occupied, without much need to

access sites and services based overseas—assuming they have no interest in politics, religion, or human rights issues. Baidu, the homegrown search engine, enables people to locate all the content on the Chinese-language Internet that their government permits. The social networking platforms RenRen and Kaixinwang substitute for Facebook. People can blog on platforms run by Chinese companies like Sohu and Sina, which also runs a wildly popular Twitter-like microblogging service, Weibo. QQ, run by the company Tencent, offers instant messaging, gaming, and all kinds of interactive services that work seamlessly across both PCs and mobile phones. These companies have all benefited from substantial Silicon Valley investment over the past decade, and many are listed on US stock exchanges or others outside of China. Thanks to the many Americans who find China's rapidly growing Internet market to be an irresistible investment opportunity, these companies are well funded to provide highly entertaining and useful—albeit censored and heavily monitored—content and services.

These domestic companies are the stewards and handmaidens, the tools and enforcers, of China's inner layer of Internet censorship. Why simply block content when you can delete it from the Internet for good? Why hire government employees to carry out censorship and surveillance when companies can be compelled to do it? The government requires companies operating inside China to use a combination of computer algorithms as well as human editors to identify objectionable material and remove it from the Internet completely. Companies that fail to obey government orders face different grades of punishment: from warnings or stiff fines to temporary shutdowns or revocation of the company's business license. Many thousands of Chinese websites and dozens of companies have been shuttered because they failed to control their content adequately.

This requirement of corporate self-censorship applies to all Chinese websites, from small online communities to the largest commercial sites, like Baidu. It also applies to all foreign Internet companies with operations inside China—including Google.cn before Google decided to pull out. Google's experience with Chinese censorship helps illustrate how

these different layers work. Before it entered China in 2006, Google operated outside the "great firewall," which means that it was subject to blocking by the Chinese network. For example, if one were on the Internet in China and typed the Chinese characters for something politically uncontroversial, say, "automobile," into the search box on Google.com, everything would work fine. But if you tried to search for anything politically sensitive—such as the Chinese phrase for "Tiananmen Square massacre" or something related to politically sensitive breaking news, like the name of a city where a riot had just occurred—the page would be blocked. The page existed on a server overseas, but it could not be viewed in China. In other words, the search was blocked not by Google but by Chinese network engineers.

Then in 2006, Google decided that subjecting users to the inconvenience and frustration of such increasingly frequent blockages was not the best way to attract Chinese Internet users to its search engine. So they launched Google.cn inside China, agreeing to abide by the Chinese government's censorship requirements. To gain permission to operate from within the firewall, Google had to agree to adjust its search algorithms so that results on Google.cn would not include websites blacklisted by the Chinese government. Rather than get a blank page when searching for the Chinese name of a city where a riot had recently been put down by police, users of Google.cn would get a sanitized set of search results about that city, minus web pages containing reports from human rights and dissident websites.

After Google announced in January 2010 it was reconsidering its business in China, then pulled its search engine out of China in March, the government imposed strict media controls on the story. As a first line of defense, the "great firewall" blocked overseas Chinese-language news reports about Google's decision to remove its search engine. The government also deployed a range of offensive tactics: all blog-hosting services, microblog platforms, and social networking services operating inside China were required to censor what Chinese Internet users said about Google. Authorities issued specific instructions to spin and manipulate the domestic media, in an aggressive effort to shape public

opinion about what had happened. Not that people could not say anything; they were free to show Google in a negative light, and there were plenty of Chinese Internet users happy to trash Google, as there are all over the world.

But Chinese bloggers and social network users who expressed sympathy for Google's situation quickly found their postings deleted and blocked by all Internet companies—domestic and foreign—operating inside China. Writings by liberal-leaning people who argued that the free flow of information would be better for China's economy and that censorship only makes it harder for the Chinese government and people to resolve problems were also deleted. The government's State Council Information Office issued a direct and detailed order on the subject to all websites and news organizations. A Chinese blogger obtained the full text and posted it online. Here is a portion of that text, translated by the California-based website *China Digital Times*, run by the exiled activist Xiao Qiang:

1. It is not permitted to hold discussions or investigations on the Google topic.
2. Interactive sections do not recommend this topic, do not place this topic and related comments at the top.
3. All websites please clean up text, images and sound and videos which attack the Party, State, government agencies, Internet policies with the excuse of this event.
4. All websites please clean up text, images and sound and videos which support Google, dedicate flowers to Google, ask Google to stay, cheer for Google and others have a different tune from government policy.
5. On topics related to Google, carefully manage the information in exchanges, comments and other interactive sessions.
6. Chief managers in different regions please assign specific manpower to monitor Google-related information; if there is information about mass incidents [the Chinese euphemism for "protests"], please report it in a timely manner.

Such directives are common, forcing Internet companies to maintain entire departments full of people whose job it is to respond to them. In late December 2010, Wang Chen, deputy head of the Communist Party's propaganda department and chief of the State Council Information Office—two of several party and government bodies in charge of Internet censorship policies—boasted in a speech that 350 million pieces of "harmful content" had been deleted from the Chinese Internet over the course of one year. Earlier that year, in a presentation to top government leaders, Wang gave a detailed description of an Internet "management system that integrates legal regulation, administrative supervision, industry self-regulation, and technological safeguards." Some sections of his speech (the full text of which was leaked to the New York-based group Human Rights in China) were deleted from the publicly released version. One of these deleted sections, which the government did not intend to share with the public, said:

We are following the overall thinking of combining Internet content management with industry management and security supervision; combining prior review and approval with supervision afterwards; combining technological blocking with public opinion guidance; combining hierarchical management with local management; combining government management with industry self-regulation; and combining online monitoring with offline management.

In such an environment where search engines and social networking services are so heavily censored, most people are not even aware of the existence of many facts, incidents, or ideas unless somebody they know who is technically savvy enough to access uncensored online spaces happens to e-mail a link to them. People who use domestic e-mail services and social networking platforms to disseminate such information, of course, are subject to monitoring and potential arrest. Data-mining software and "deep packet inspection" technologies make it easy to automate surveillance through the Internet service providers and

mobile carriers of all unencrypted Internet traffic no matter what service is being used or where it is based.

In 2011, the government moved to extend these censorship and surveillance mechanisms, as well as to improve their coordination. In March 2011, spooked by the Arab Spring, the central government established a new overarching government agency responsible for controlling all Internet platforms and services. The number of censored foreign websites, social networking platforms, and even data-hosting and "cloud computing" services expanded dramatically. Surveillance systems were upgraded to more aggressively track and identify Chinese citizens who managed to circumvent the blockages to use tools like Twitter. It became commonplace for Twitter users to be questioned about their postings, and at least one person was arrested for no other reason than a tweet she had sent out.

AUTHORITARIAN DELIBERATION

At 5 a.m. July 16, 2009, Guo Baofeng, a young entrepreneur who lives in the city of Mawei in the southern coastal province of Fujian, posted two short messages in English onto Twitter from his Blackberry:

*Pls help me, I grasp the phone during police sleep
I have been arrested by Mawei police, SOS*

Guo's tweets, sent furtively before police confiscated his phone, were quickly retweeted by hundreds of people in China and around the world. Nothing more was heard from him, but those short tweets were enough. People in his Twitter network who knew his real-life identity followed up with his family and friends in Mawei. News quickly spread around Twitter that the police had taken Guo from his office the previous afternoon.

Along with several other bloggers, Guo was arrested on defamation charges, after posting information online about the alleged gang rape and murder by local officials of a young woman named Yan Xiao-

ling. News of Yan's case had spread virally in chat rooms and blings after the young woman's parents insisted she was violently raped, contradicting police claims that she died from a hemorrhage caused by an ectopic pregnancy. Authorities scrambled to stop the further spread of allegations online. The Communist Party's propaganda department instructed news outlets and social media websites to delete all discussion of Yan's case, but some people like Guo continued passing around the news on foreign social media platforms like Twitter to reach those few hundred thousand Chinese users who know how to circumvent the firewall.

Guo's Twitter followers immediately began to rally for his release. One well-known Guangzhou-based blogger named Wen Yunchao called for a postcard-writing campaign to shame authorities into releasing him. Hundreds of people mailed postcards to the Fuzhou detention center where Guo was being held, with the simple message: "Guo Baofeng, your mother wants you home for dinner." Others organized a fund-raising drive to pay for his defense. After sixteen days in detention, Guo and two other bloggers who had been arrested around the same time were released. "I used Twitter to save myself," he wrote on his blog. The massive online reaction, he believes, helped to free him.

The people who rallied to free Guo did not spring immaculately from cyberspace—or from Twitter. Many of them had gotten to know one another both online and offline over the course of several years through a loose community of liberal-thinking, internationalist-minded bloggers, web developers, and entrepreneurs. For five years beginning in 2005 they even held annual conferences. They were, in essence, the reformist, prodemocracy branch of China's digital commons. In November 2009, the Sichuan-based writer Ran Yunfei stood in front of several dozen liberal Chinese bloggers at the fifth annual Chinese Blogger Conference, held in the small town of Lianzhou, Guangdong province, and explained how vital it is that people continue speaking their minds online. "As we use the Internet every day, it changes us. It has made me more tolerant and taught me to play by a set of rules. . . . As we train ourselves we are also training the government. . . . Hopefully one day

they will understand that they don't need to be afraid of us, that we can all legally and rationally coexist."

The Chinese Communist Party acted aggressively in 2010 and 2011 to smash all dreams of any such coexistence. When the same group of bloggers tried to organize another gathering in November 2010, police threatened organizers, and what would have been the sixth annual Chinese Blogger Conference was canceled. In early 2011, after the Tunisian and Egyptian governments fell to popular uprisings that came to be known as the "jasmine revolution," calls for "jasmine" protests in China began to circulate in the Chinese twittersphere. Ran Yunfei was arrested and charged with subversion, although he appeared to have done nothing more than to retweet some controversial messages about events in Tunisia and Egypt, with comparisons to China. Other members of the liberal Chinese blogger community—many of whom had also signed Liu Xiaobo's Charter 08 two years previously—were detained for days or weeks. Many more were questioned by the police and warned that they were being closely watched. Transcripts of people's posts on Twitter and on other social media platforms featured in interrogation sessions. China's liberal reformist commons was quashed. Thanks to censorship, most educated Chinese people never knew this community existed.

Herein lies the paradox of the Chinese Internet: public debate and even some forms of activism are expanding on it, while at the same time, state controls and manipulation tactics have managed to prevent democracy movements from gaining meaningful traction. Min Jiang, a scholar of the Chinese Internet at the University of North Carolina at Charlotte, calls this sort of lively but limited public discourse "authoritarian deliberation." Her argument centers around the idea—often overlooked by Western punditry—that it is possible for a large amount of public debate, and even some kinds of policy activism, to exist within the confines of an authoritarian state. A major difference between democratic and authoritarian deliberation is that in the authoritarian context, the state sets limits to political speech. The state conducts surveillance against which citizens have no legal recourse. The right to free expression is not guaranteed and cannot be defended in court because the ju-

dicial system is not independent. But thanks to the Internet, people have vastly more room to voice their concerns and criticize public authorities than ever before—even in China.

Chinese government officials and the state-run media actually talk about Chinese-style "Internet democracy" as an alternative to "Western-style" multiparty democracy. China's parliament now has an "e-parliament" website, on which it invites members of the public to make policy suggestions. Outsiders who do not read Chinese or follow China's Internet scene closely would be very surprised to learn about some of the suggestions people are allowed to post. People post detailed suggestions on a range of subjects, such as reducing local corruption, improving the environment, and proposing financial reforms. In 2009, the first year the e-parliament was launched, somebody posted a long treatise about why China's one-child population-control policy should be scrapped. In the comments thread following the posting, a long argument ensued among people from across the country, some supporting the policy's abolition, others defending it as a key to China's economic success, and still others accepting some kind of population-control policy but proposing that the current one be made more flexible.

As it happens, for the past several years the central government has been modifying China's one-child policy as the population ages and the birth rate drops, making such conversations useful in gauging potential public reactions to policy changes. At the same time, attempts to post proposals for multiparty electoral reform on the e-parliament website will be censored. But the government nonetheless points to such websites to demonstrate that it is listening to public opinion and taking it seriously. They even quote President Hu Jintao, who gave his blessing to the whole enterprise back in 2008 when he said to the *People's Daily*, "The web is an important channel for us to understand the concerns of the public and assemble the wisdom of the public."

Since President Hu made those remarks and conducted his first public web chat, Chinese leaders at all levels have been bolding regular online chats with the public. Officials at all levels of government—even police chiefs in some cities—have set up public accounts on Weibo, the

Chinese version of Twitter, to demonstrate an interest in public opinion as well as to help the public better understand their priorities. Of course, the various online platforms through which the public is invited to converse with officials are policed and censored. Postings that might contain serious critiques of the whole system, or that call for political reform, are eliminated.

Thus the Chinese government can maintain an authoritarian state, while at the same time the Internet enables a high level of lively and even contentious online debate and deliberation, within certain limits. After a July 2011 high-speed-rail crash in the city of Wenzhou that killed at least forty people and injured nearly two hundred, Chinese Internet users were able to use Weibo to tweet a stream of on-the-scene reports as well as critical invective about corruption and malfeasance that contributed to the crash, without the Communist Party's power being fundamentally threatened. After an outburst of online rage in the immediate aftermath of the crash, the government moved to muzzle all professional media coverage and also tightened the screws on Internet companies and social networking companies to track and censor critical postings, especially any that linked the crash to broader national governance failures or attempted to organize offline responses. As a result, the spontaneous outpouring of anger—which was too big and sudden to be contained—that followed the crash was prevented from morphing into offline protests or any broader movement for political change.

Meanwhile, as the government has moved aggressively to quash the communities in the Chinese digital commons harboring people who are sympathetic to calls for political reform, government-friendly communities are allowed to thrive. Some are the product of direct manipulation but others are largely spontaneous and voluntary. To discredit liberal viewpoints in Chinese cyberspace, the government deploys other means to sway public opinion by—to use an American political and commercial marketing term—“Astroturfing” the Chinese Internet with progovernment commentary. Communist Party youth league volunteers and paid freelance recruits known derisively as the “fifty-cent party” (because they are paid roughly fifty Chinese cents per posting) lurk on

blogs and chat rooms, posting patriotic and progovernment comments and reporting on excessive political deviance. But beyond the Astroturfers, there are also many young patriotic Chinese who create online communities on their own initiative. One example is April Media, an online community of nationalist bloggers run by a young man named Rao Jin, a recent graduate of the prestigious Tsinghua University in Beijing, dedicated to exposing the Western media's “anti-China bias.”

Rao launched the site, originally titled Anti-CNN, in March 2008 in the wake of ethnic unrest and the subsequent Chinese government crackdown in Tibet. Western media coverage of the news included highly critical commentary of the Chinese government, including a comment by CNN commentator Jack Cafferty calling them “goons and thugs.” (Cafferty and CNN later apologized.) Editors of major Western TV broadcasters also made serious errors in their coverage of the unrest and crackdown in Tibet, confusing photos of protests in India and Nepal with protests in Tibet. Rao and his team of young students believed that these errors were not innocent mistakes but instead represented an international media conspiracy against China. The website's first posting, devoted to media errors, generated over 200,000 hits, a long thread of comments, and hundreds of angry young people willing to volunteer their time to help monitor, translate, and analyze what the Western media was reporting about China. When I visited his office in 2009, Rao insisted that the site was not meant to be antiforeign or anti-Western, just anti-Western media, which he believes view China “through colored lenses.”

Renamed April Media in 2009, the site has continued to fuel critiques on Chinese social media platforms about Western news coverage of other major events. In February 2011 a member of Rao's online community spotted US ambassador John Huntsman on the edge of a crowd near a Beijing McDonald's that just happened to have been designated as a protest spot by people trying to emulate the “jasmine” revolutions of North Africa. April Media wasted no time in disseminating a viral video showing footage of the indignant Chinese netizens confronting the US ambassador. The video ended with a commentary condemning the

United States for interfering in other countries' affairs, and warning that the United States could turn China into yet another Iraq if the Chinese people were not vigilant. The government had no direct hand in this act of "citizen journalism" or the video; it was a spontaneous product of China's nationalist commons.

The motivations of Rao's band of young, nationalistic media activists are similar to those of China's patriotic hackers—often loose alliances of computer whizzes who engage in patriotic hacking missions, and whose relationship to the government is often unclear. In 2009, a team of information warfare researchers affiliated with the University of Toronto uncovered a cyber-espionage network they dubbed "GhostNet," involving at least 1,295 infected computers in 103 countries. They discovered that the Trojan software used to infect these computers was controlled by commercial Internet accounts in China's Hainan province. Targets included the private offices of the Dalai Lama and other exiled Tibetan organizations and offices, from which sensitive and secret information was stolen.

The GhostNet report authors pointed out that it was impossible to prove that the attacks had been organized or carried out by the Chinese government; the best they could do was trace them to a location on China's Hainan Island. Security specialists who study Chinese hacker culture have found that even as government and military cyber-defense and cyber-warfare units have developed and matured, a great deal of freelance hacking continues to be directed at the People's Republic of China's perceived adversaries—with varying degrees of communication (or compensation) taking place between the hackers and Chinese military, state security, or other Communist Party entities. This hacker netherworld works to the government's advantage, providing deniability as well as greater flexibility, in addition to being a ready-made channel for recruitment into real government jobs in the military and security services. In a 2007 book about China's patriotic hacker communities based on several years of in-depth research, security expert Scott Henderson concluded that the bulk of the cyber-attacks taking place up until that time had been conducted by groups of young hack-

ers who had formed into clubs, and of whom the government made both direct and indirect use. "In Chinese society, independence from government direction and control does not carry with it the idea of separation from the state," Henderson wrote. "The PRC government views its citizenry as an integral part of Comprehensive National Power and a vital component to national security." Online communities like Rao Jin's are the "citizen media" equivalent of this phenomenon.

WESTERN FANTASIES VERSUS REALITY

When the United States first began to engage China politically and economically in 1979, many Washington policy makers assumed that capitalism would inevitably bring democratization. Reality has played out differently. Capitalist investors are actually helping the Chinese Communist Party strengthen and refine a gilded cage for China's Internet users. This cage is made as large and exciting as possible for the Chinese people, plying them with ever more digital conveniences, delights, comforts—and even outlets for political debate, giving people the sense that they are much more free than ever before, as long as they do not cross certain lines.

The government cannot afford to sever links between the domestic Chinese Internet and the international Internet without disrupting the international business, trade, and finance upon which its economy now depends. Thanks in part to copious foreign investment, however, the domestic Internet has grown robust and useful enough for the majority of Chinese Internet users that the government has been able to restrict access to the global Internet without widespread public outcry. In early 2011, government network engineers gave the "great firewall" a major upgrade, blocking some of the Internet protocols used to establish secure and encrypted connections and making it much more difficult than ever for people to use virtual private network services to circumvent censorship and evade surveillance. Access to Gmail and a number of other popular international services was not fully blocked but was slowed down to make the sites more difficult to access without delays and

connection errors. University and corporate networks suffered disruptions as "punishment" when individual users tried to use circumvention tools to access blocked websites. In May 2011, Hong Kong-based activist Oiwan Lam collected a number of warning notices from corporate and university IT departments and posted them on the Global Voices advocacy site. A typical example was this one issued by the Chinese Academy of Sciences:

Our faculty's access to overseas websites have been disrupted in the past few days. Upon investigation, the reason is because some users have used circumvention tools to get access to illegal content, hence the public security bureau has black-listed our faculty's IP. Here I remind everyone to follow the rule when using Internet, don't use illegal means to get access to illegal information!

Such measures are an extension of quiet measures implemented several years before on some university campuses. Many of China's top universities, including Peking University and Tsinghua University, provide free broadband to students in their dormitories. But there is a catch: the service is free only for domestic websites and a select set of "white-listed" overseas websites. To access any other websites or services from outside of China, students are charged according to how many megabites they upload or download. Most students, being on tight budgets, see very little of the global Internet.

Fortunately for the government, there are plenty of websites and services on the Chinese Internet to keep people occupied, without ever needing to access sites and services based overseas. Baidu helps them locate all the content on the Chinese-language Internet that their government permits. Social networking platforms RenRen and Kaixin-wang substitute for Facebook. People can blog on platforms run by Chinese companies like Sohu and Sina and "tweet" on Weibo. QQ, run by the company Tencent, offers instant-messaging, gaming, and all kinds of interactive services that work seamlessly across both PCs and mobile phones.

Chinese Internet company executives occasionally complain about being forced to censor and track users, but insidiously, their business is too profitable to resist. They are too deeply invested and complicit, as are their international investors. According to the Boston Consulting Group, China's e-commerce market is expected to soon become the world's largest, quadrupling from \$71 billion in 2010 to a projected \$305 billion in 2015. The amount of money raised by Chinese venture funds—much of it for Internet start-ups—grew from almost \$4 billion in 2006 to more than \$11 billion in 2010. China's three largest Internet companies, Tencent, Baidu, and Alibaba, are all listed on overseas stock markets. So are several other major Internet brands including RenRen, a social networking platform similar to Facebook, which raised \$743 million in its IPO on NASDAQ in early May 2011.

The more successful and popular these companies become, the less incentive Chinese Internet users will have to access blocked foreign services like Facebook, Twitter, or YouTube—beyond a small politically motivated cohort, who are always a small minority of any country's population. It will also become easier to restrict general access to the international Internet without a widespread public outcry. The restriction in turn boosts the traffic and advertising revenue for Chinese Internet companies, making them all the more attractive to foreign investors.

When commercial Internet service first became available in China in 1995, Western policy makers and journalists—myself included—made very different assumptions about how the Internet would change China. In explaining the de-linkage between human rights standards and China's "most-favored nation" trading status in 1994, US Secretary of State Warren Christopher reinforced this assumption when he declared, "Economic development depends upon the free flow of information; computers are the new vehicles of political expression. The software of freedom will, ultimately, prevail over the hardware of repression." Washington policy makers and the US business community failed to anticipate the extent to which the Chinese government could compel domestic and foreign companies to rewrite the software and rewire the hardware to the Chinese Communist Party's specifications.

The Chinese Communist Party has created a system that keeps itself in power while engaging its citizens and helping them succeed economically. The private sector has a stake in maintaining and reinforcing this system with the enthusiastic support of American investors who also profit from its existence. Unless and until a critical mass of Chinese Internet users decide that the status quo is unacceptable and demand access to alternatives beyond their "gilded cage," and unless Chinese entrepreneurs and CEOs decide that it is in their long-term interest to help build a different kind of future, more than likely the Internet's pervasive use in China will actually help *prolong* the Communist Party's rule of China rather than hasten its demise. The implications of this reality extend well beyond China.

CHAPTER 4

Variants and Permutations

When the Egyptian government shut down the Internet on January 27, 2011, it was a serious wake-up call to activists and opposition groups around the world, many of whom had never before fully considered the implications of both government and corporate control over a nation's digital networks. The Egyptian government was able to shut down the Internet relatively easily for two key reasons: First, the government controls the limited number of fiber-optic links going in and out of the country, and the state-owned telecommunications company leases access to them by ISPs. So even if an ISP were to keep its internal links running, the reliance of so many local web and e-mail operations on overseas hosting and domain services means that even most domestic websites cannot load and e-mails cannot be sent within the country when the government cuts off international access. Second, licensing agreements required by the government of all Internet service providers—including foreign companies such as Vodafone—left those companies without legal grounds to challenge a government shutdown order.

Though total Internet shutdown is a drastic measure, it had already been used elsewhere: in Burma during the attempted "saffron revolution" in 2008. In 2009, China shut down the Internet for the entire province of Xinjiang in the country's far Northwest for nearly six months after ethnic riots erupted there. Iran did not shut down the Internet completely during the 2009 postelection Green Movement protests but