# RESET

sept
em
b
er

A sample chapter from
September Publishing

ALSO BY THE AUTHOR

*Black Code: Surveillance, Privacy, and the Dark Side of the Internet*

*Parchment, Printing, and Hypermedia: Communications in World Order Transformation*

Ronald J. Deibert

# RESET.

## Reclaiming the Internet for Civil Society

september

1 3 5 7 9 10 8 6 4 2

This paperback published in the UK in 2021 by September Publishing
Ebook published in the UK in 2020 by September Publishing
First published in Canada and the USA in 2020 by
House of Anansi Press Inc.

Text design: Ingrid Paulson

Paperback ISBN 9781912836772
Kindle ISBN 9781912836789
Epub ISBN 9781912836796

September Publishing
www.septemberpublishing.org

For Jane:
my love, my lifeline,
my morning coffee confidante

# CONTENTS

“Constant experience shows us that every man invested with power is apt to abuse it, and to carry his authority as far as it will go . . . To prevent this abuse, it is necessary from the very nature of things that power should be a check to power.”

Montesquieu, *The Spirit of Laws*

# INTRODUCTION

LOOK AT THAT DEVICE in your hand.

No, really, take a good, long look at it.

You carry it around with you wherever you go. You sleep with it, work with it, run with it, you play games on it. You depend on it, and panic when you can't find it. It links you to your relatives and kids. You take photos and videos with it, and share them with friends and family. It alerts you to public emergencies and reminds you of hair appointments.

*Traffic is light. If you leave now you will be on time.*

You depend on it for directions, weather forecasts, and the news. You talk to it, and it talks back. You monitor the appliances that in turn monitor your house (and you) with it. You book your flights on it and purchase your movie tickets through it. You order groceries and takeout and check recipes on it. It counts your steps and monitors your heartbeat. It reminds you to be mindful. You use it for yoga and meditation.

But if you're like most everyone I know, you also probably feel a bit anxious about it. You realize it (and what it connects you to) is doing things to your lifestyle that you'd probably be better off without. It's encouraging bad habits. Your kids and even some of your friends barely talk to you in person any longer. Sometimes it feels like they don't even look you in the face, their eyeballs glued to it, their thumbs tapping away constantly. Your teen freaks out when their device rings. *You mean I have to actually speak to someone?* How could something so "social" be also so curiously anti-social at the same time?

You check your social media account, and it feels like a toxic mess, but you can't help but swipe for more. Tens of thousands, perhaps millions, of people actually believe the earth is flat because they watched videos extolling conspiracies about it on YouTube. Right-wing, neo-fascist populism flourishes online and off, igniting hatred, murder, and even genocide. A daily assault on the free press rains down unfiltered from the Twitter account of the president of the United States, whose brazen lies since taking office number in the tens of thousands. His tweets are symptomatic of the general malaise: like a car accident, they are grotesque, but somehow you are drawn in and can't look away.

No doubt you have also noticed that social media have taken a drubbing in recent years. The "gee whiz" factor has given way to a kind of dreadful ennui. Your daily news feeds fill with stories about data breaches, privacy infringements, disinformation, spying, and manipulation of political events. Social media executives have been dragged before congressional and parliamentary hearings to face the glare of the cameras and the scrutiny of lawmakers.

The 2016 Brexit referendum and the 2016 U.S. election of president Donald Trump were both major precipitating factors behind the re-examination of social media's impact on society and politics. In both cases, malicious actors, domestic and foreign, used social media to spread malfeasance and ignite real-life protests with the intent to foster chaos and further strain already acute social divisions. Thanks to investigations undertaken in their aftermath, shady data analytics companies like Cambridge Analytica have been flushed out from the shadows to show a glimpse of social media's seamy underworld.

Then there's the *real* dark side to it all. You've read about high-tech mercenary companies selling powerful "cyberwarfare" services to dictators who use them to hack into their adversaries' devices and social networks, often with lethal consequences. First it was Jamal Khashoggi's inner circle, then (allegedly) Jeff Bezos's device. *Maybe I've been hacked too?* you wonder to yourself, suddenly suspicious of that unsolicited text or email with an attachment. The world you're connecting to with that device increasingly feels like a major source of personal risk.

But it's also become your lifeline, now more than ever. When the novel coronavirus (2019-nCoV or COVID-19) swept across the globe after its discovery in

Wuhan, China, in December 2019, business as usual ground to a halt: entire industries shuttered, employees laid off in the millions, and nearly everyone forced into self-isolation and work-from-home. While all other sectors of the global economy were on a rapid downward spiral, the large technology platforms saw use of their services skyrocket. Video conferencing tools, like Zoom, went from obscure office contrivances to something so commonplace your grandparents or children used it, often for hours on end. Netflix, Amazon Prime, and other streaming media services were booming, a welcome distraction from the grim news outside. Bandwidth consumption catapulted to such enormous levels that telecommunications carriers were putting caps on streams and downgrading video quality to ensure the internet didn't overload. Miraculously, it all hung together, and for that you were grateful.

But the global pandemic also accentuated all of social media's shortcomings. Cybercrime and data breaches also skyrocketed as bad actors capitalized on millions of people working from home, their kitchen routers and jerry-rigged network setups never designed to handle sensitive communications. In spite of efforts by social media platforms to remove misleading information and point their users to credible health sources, disinformation was everywhere, sometimes consumed with terrible effects. People perished drinking poisonous cocktails shared over social media (and endorsed by Donald Trump himself) in a desperate attempt to stave off the virus.

The entire situation presented a striking contrast both to the ways in which social media advertise themselves and to how they were widely perceived in the past. Once, it was conventional wisdom to assume that digital technologies would enable greater access to information, facilitate collective organizing, and empower civil society. The Arab Spring, the so-called "coloured revolutions," and other digitally fuelled social movements like them seemed to demonstrate the unstoppable people power unleashed by our always-on, interconnected world. Indeed, for much of the 2000s, technology enthusiasts applauded each new innovation as a way to bring people closer together and revitalize democracy.

Now, social media are increasingly perceived as contributing to a kind of social sickness. A growing number of people believe that social media have a disproportionate influence over important social and political decisions. Others are beginning to notice that we are spending an unhealthy amount of our lives staring at our devices, "socializing," while in reality we are living in isolation and detached from nature. As a consequence of this growing unease, there are calls to regulate social media and to encourage company executives to be better stewards of their platforms, respect privacy, and acknowledge the role of human rights. But where to begin? And what exactly should be done? Answers to these questions are far less clear.

THE TITLE OF THIS BOOK, *Reset,* is intended to prompt a general stocktaking about the unusual and quite disturbing period of time in which we find ourselves. "The arc of the moral universe is long, but it bends toward justice," Martin Luther King Jr. once famously observed. Looking around at the climate crisis, deadly diseases, species extinction, virulent nationalism, systemic racism, audacious kleptocracy, and extreme inequality, it's really hard to share his optimism. These days it feels more like everything's all imploding instead. If there has ever been a time when we needed to rethink what we're collectively doing, this is certainly it.

More specifically, the title is also intended to signal a deeper re-examination of our communications ecosystem that I believe is urgently required, now more than ever. In the language of computers and networking, the term "reset" is used widely to refer to a measure that halts a system and returns it to an initial state. (The term "reboot" is often used interchangeably.) A reset is a way to terminate a runaway process that is causing problems and start over anew. Users of Apple products will be familiar with the "spinning beach ball" that signifies a process that is stuck in a loop, while Microsoft customers will no doubt recall the "blue screen of death." We've all been there at one time or another.

The term "reset" is also used more broadly to refer to a fresh start. As when parents tell their children to take a "time out," a reset is usually suggested when something we are doing has become counterproductive and deserves some reconsideration. It's also common to think about a reset when we do something entirely novel, like begin a new job or move to a new house. Resets allow time to regroup, clean house, take stock and look at the big picture, and launch a new plan. In broader parlance, a reset implies beginning again from well-thought-out first principles. It allows us to discard the errors of the old ways of going about things and start over with a solid foundation.

During the COVID emergency, societies were compelled into an unexpected and enforced reset. Governments around the world, from the municipal to the federal level, mandated quarantines and self-isolation protocols. The global economy effectively went into an indefinite pause as entire sectors were shut down. Emergency measures were introduced. At the time of writing, in spring 2020, we were still at a relatively early stage of the pandemic's spread, and it's unclear how everything will resolve. However it all turns out, the enforced time out has prompted a re-examination of many aspects of our lives and our politics, and social media are certainly not exempt.

I have several objectives in writing *Reset*. One aim is to synthesize what I see as an emerging consensus about the problems related to social media and — by extension — the organization of our entire communications environment. Think of this as a diagnosis of social media: an identification of the illnesses by a close examination of their symptoms. I organize these problems as "painful truths" — "truths" because there is a growing number of scholars and experts who acknowledge these problems, and "painful" because they describe many serious and detrimental effects that are unpleasant to contemplate and difficult to fix. In doing so, I am not so much putting forward a single original argument about social media as combining a lot of disparate research and reporting undertaken by many others who have studied the topic. Of course, not everyone will agree with my synthesis or characterization of these problems. But I have tried as much as possible to capture what I see as the latest evidence-based research and thinking on the topic — to provide a comprehensive picture of the state of the art at the time of writing.

*Reset* is, therefore, not intended solely for a specialist audience, and it is not sourced in the same manner as a peer-reviewed academic book on the topic would be. I have tried to make *Reset* as accessible as possible, while still being faithful to the recent scholarship on the topic. For those who wish to get into the weeds a little bit more, and to give credit where credit is due, alongside this book I am publishing a detailed bibliography of sources. I feel as though I am part of a large community of scholars who have spent their professional lives dissecting these painful truths about social media — scholars like Rebecca MacKinnon, Tim Wu, Zeynep Tufekci, Siva Vaidhyanathan, danah boyd, Kate Crawford, Bruce Schneier, Ryan Calo, and many others too numerous to list here. In describing the painful truths about social media, I hope to be able to help convey those thinkers' collective concerns as accurately as possible.

Another aim of this work is to move beyond these painful truths and start a conversation about what to do about them. There is a very long and growing list of books, articles, and podcasts that lay bare the problems of social media, but few of them offer a clear alternative or a path forward. Those solutions that are proposed can feel fragmented or incomplete. At best, one might find a few cursory platitudes tacked on in the final paragraphs of an essay or book that hint at, but don't elaborate on, what to do. That is not to say there is a shortage of proposals to reform social media in some fashion; those are plentiful but can also be confusing or seemingly contradictory. Should we break up Facebook and other tech giants, or reform them from within? Should we completely unplug and disconnect, or is there a new app that can help moderate the worst excesses of social media?

My aim is to bring some clarity to this challenge by laying out an underlying framework to help guide us moving forward. However much it may feel like we are in uncharted territory, I don't believe we need to invent some new "cyber" theory to deal with the problems of social media (and we certainly can't pin our hopes on a new app). Humans have faced challenges in other eras similar to our own. We have done this before, albeit at different scales and under different circumstances. There is, in fact, a long tradition of theorizing about security and liberty from which we can draw as we set out to reclaim the internet for civil society. I hope to elaborate on what I see as some of the most promising elements of that tradition.

NOT THAT LONG AGO—and I mean within my adult life—we used information and communications technologies self-consciously and as deliberate one-off acts. We made a telephone call. We watched television. We listened to the radio. We dropped a letter in the postbox. Later, we composed essays or undertook calculations on our desktop computers. These were all relatively self-contained and isolated performances, separate from each other and from other aspects of "normal life." But beginning around the 1980s (at least for those of us living in the industrialized West), things began to change quickly. Those desktop computers were eventually networked together through the internet and internet-based subscription services like CompuServe or America Online. The World Wide Web (1991) brought a kind of Technicolor to the internet while unleashing a dramatically new means of individual self-expression. Thanks to improvements in cellular technologies and miniaturized transistors, telephones went mobile. Before long, Apple gave us the iPod (in 2001), onto which we could download digital music. The iPhone (released in 2007) combined the two and then integrated their various functions via the internet, producing a one-stop, all-purpose, mobile digital networking "smart" device.

Before long, the internet was in everything, from wearables and networked kitchen appliances all the way down to the molecular level with digitally networked implants, like pacemakers and insulin pumps. (Perhaps not surprisingly, security experts have routinely discovered potentially life-threatening software vulnerabilities in many versions of the latter.) Digitally networked neural implants that are presently used for deep-brain and nerve stimulation, as well as to enable mind-controlled prosthetics, are merely at the rudimentary stages of development; engineers are experimenting on systems involving thousands of tiny speck-sized neural implants that would wirelessly communicate with computers outside the brain. Whatever the future brings, we are all now "cyborgs" — a term that once described a hypothetical fusion of "human" and "machine." One can no longer draw a clear separation between our "normal" and our "digital" lives (or, to use older lingo, between "meat" and "virtual spaces"). Our use of information and communications technologies is now less a series of deliberate, self-conscious acts and more like something that just continuously runs in the background. Much of it is rendered invisible through familiarity and habituation. Disparate systems have converged into an always-on, always-connected mega-machine. This profound shift in how we communicate and seek and receive information has occurred largely within the span of a single generation.

To be sure, there is still vast digital inequality (nearly half of the world's population has yet to come online), but those gaps are closing quickly. The fastest growth in mobile internet connectivity is in the global South, as entire populations leapfrog over older legacy systems and "fixed line" connections to plug directly into social media using mobile devices. But the uses towards which those populations (and all next-generation users, for that matter) are putting digital technologies are sometimes quite surprising, and different than what the original designers intended. Human ingenuity can reveal itself in many unexpected ways. The internet gave us access to libraries and hobby boards, but also gave criminal enterprises low-risk opportunities for new types of global malfeasance, like spam, phishing schemes, and (more recently) ransomware and robocalls. Early in the internet's history, many assumed the technology would hamstring dictators and despots, and, to be sure, it has created some control issues for them. But it's also created opportunities for older practices to flourish, such as the way "*kompromat*" (Russian for "compromising material used for blackmail and extortion") has taken on new life in post-Soviet social media. The entire ecosystem was not developed with a single well-thought-out design plan, and security has largely been an afterthought. New applications have been slapped on top of legacy systems and then patched backwards haphazardly, leaving persistent and sometimes gaping vulnerabilities up and down the entire environment for a multitude of bad actors to exploit. It's all an "accidental megastructure," as media theorist Benjamin Bratton aptly put it.

The global communications ecosystem is not a fixed "thing." It's not anywhere near stasis either. It's a continuously evolving mixture of elements, some slow-moving and persistent and others quickly mutating. There are deeper layers, like those legacy standards and protocols, that remain largely fixed. But caked on top of them is a bewildering array of new applications, features, and devices. Weaving through it all are rivers of data, some neatly contained in proper channels, others pouring through the cracks and crevices and spilling out in the form of data breaches. The phrase "data is the new oil" refers to the value to be gained from all the data that is routinely harvested by machines from both humans and other machines — the entire complex bristling with millions of pulsating data-sorting algorithms and sensors. The gradual rollout of fifth-generation cellular technology, known as 5G, will dramatically increase the speed and broadband capacity of cellular networks, fuelling an even greater volume of data circulating among a larger number of networked devices. The combined effect of each of us turning the most intimate aspects of our digital lives inside out has created a new emergent property on a planetary scale that has taken a life of its own — derived from but separate from us, a datasphere.

"Social media" (strictly understood) refers to the breed of applications that emerged in the past decade and a half, thanks largely to the extraordinary business innovations of Google and Facebook, and gave rise to what the political economist and business management professor Shoshana Zuboff has termed “surveillance capitalism.” Merriam-Webster defines social media narrowly as “forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos).” But missing from this definition is the underlying business model, an appreciation of which is essential in order to fully understand the dynamics of social media. At their core, social media are vehicles for the relentless collection and monetization of the personal data of their users. Social media are so overwhelming and omnipresent in our lives, it may feel like they have been with us forever. Some of you reading this may have grown up entirely within the universe of Facebook, Google, Snapchat, and TikTok and not know what it's like to live without them. I'm among those living generations that have experienced life before and after social media. I remember standing in a long line with nothing to do but think.

Not everything is social media, but social media influence everything else, so prominent and influential is the business model at their core. The platforms that run social media have huge gravitational force and sweep up most everything else into their orbit (sometimes literally, through acquisitions), absorbing even non-social applications into the galaxy of social media. For example, narrowly understood, drones are not a form of social media. But both developed out of a common family of electronics, robotics, miniaturization, and digitization. Each drone is controlled by software-based, networked applications installed on handheld devices and tablets. The most popular drone is manufactured by a China-based company called DJI, whose apps send data on trips, models, locations, and more to its Shenzhen-based servers as well as numerous advertising firms and other third parties. Much like everything else these days, the influence of social media's business model has infected those applications, and so they too are oriented around personal data surveillance. Overhead remote sensing data are also integral to the functioning of many social media applications, such as Google's maps.

Social media do not stand alone. They are embedded in a vast technological ecosystem. In order to participate in social media, you need some kind of networked device: a smartphone, tablet, laptop, or PC. (The number of networked devices is expanding quickly with 5G networks and the so-called Internet of Things, and now includes internet-enabled fridges, home security systems, dishwashers, and automobiles.) Those devices send electronic signals through radio waves or cables that are transmitted through a physical infrastructure of routers, servers, cell towers, and data farms, in some cases spread throughout multiple countries. Each of these elements is operated by numerous businesses, which can include internet service providers (ISPs), cable companies, cell service providers, satellite services, undersea cable providers, and telecommunications firms as well as the various hardware and software manufacturers supporting them all. Which companies operate the various components of this ecosystem, and according to whose rules, matters enormously for users' security and privacy. For example, policymakers and analysts have raised concerns that China-based communications routing equipment manufacturers Huawei and ZTE may have designed secret "back doors" in their technology that would provide China's security agencies with an intelligence toehold in 5G networks. However valid, these concerns are not unique to China or China-based companies. The history of communications technologies is full of episodes of governments of all sorts cajoling or compelling companies that operate the infrastructure to secretly turn over data they collect. (A decade from now, we'll be worrying about whether the companies that control our brain implants have secretly inserted "back doors.")

The internet, telecommunications, and social media are so foundational to everything else that they have become an object of intense geopolitical competition among states and other actors on the world stage. "Cyber commands," "cyber forces," and "electronic armies" have proliferated. A large, growing, and mostly unaccountable private industry feeds their needs with tools, products, and services. The struggle for information advantage is a by-product of seemingly endless opportunities for data exploitation as a consequence of pervasive insecurity. Defence is expensive and difficult, so everyone goes on the offence instead. The ancient art of intelligence gathering is now a multi-billion-dollar worldwide industry that snakes clandestinely through the catacombs of the planet's electronic infrastructure. To give one illustration of the magnitude of the issue, Google's security team says that on any given day, it tracks around 250 government-backed hacking campaigns operating out of fifty countries. And yet, in spite of it all, the communications ecosystem somehow hangs together. Interdependence runs deep — even closed-off North Korea depends on the internet for illicitly acquired revenues. And so most of the offensive action (even among otherwise sworn adversaries) takes place just below the threshold of armed conflict. Subversion, psychological operations, extortion (through ransomware), and digitally produced propaganda are where the real action is to be found — less violent, to be sure, but no less destructive of the health of the global communications sphere.

The entire ecosystem requires enormous energy to power, and that in turn implicates all of the various components of the global energy grid: power stations, transmission systems, hydroelectric dams, nuclear power plants, coal-fired power plants, and others. The awesome speed with which we can send and retrieve even large amounts of data tends to obscure the vast physical infrastructure through which it all passes. Last year, my family and I did a FaceTime video call between Sydney, Australia, and Toronto, Canada, which at roughly 15,500 kilometres apart are about as distant as two points on Earth can be, and it worked seamlessly… as if it were some kind of magic. But it's not magic at all; it's physics. However immaterial they may seem, our digital experiences rest on a complex and vastly distributed planet-wide infrastructure.

To be sure, it's not all physical. This enormous communications ecosystem could not function without rules, protocols, algorithms, and software that process and order the flows of data. Some of those rules and protocols were developed decades ago and remain foundational still, like the Transmission Control Protocol and Internet Protocol (TCP/IP) underlying pretty much all internet communications, or Signalling System No. 7 (SS7), which was developed in 1975 to route telephone calls but has now unexpectedly become a major source of insecurity used to track the location of smartphones. Other rules and protocols are pasted on top as new applications are developed. Many different terms have been used to describe this entire ecosystem: the internet, cyberspace, the World Wide Web, and more. But because these can quickly date themselves, I prefer to use the more generic "communications ecosystem."

It's important to make this distinction clear, because while we may want to eliminate or temper some of the characteristics of social media, we do not necessarily want to (nor realistically can we) eliminate the vast communications ecosystem of which they are a part. Looking only narrowly at the effects of social media proper may also obscure some of the consequences connected to the broader (and continuously mutating) communications ecosystem. Throughout this book, I'll use "social media" narrowly when referring to those platforms we traditionally associate with the term, but I'll also be spending time examining other technologies connected to them that make up the communications ecosystem as a whole (like that device you hold in your hand).

THERE IS NO SHORTAGE of blame placed on social media for all sorts of social and political pathologies. But assigning causality (in a scientific sense) to social media for any particular outcome, negative or otherwise, is not always simple, given the extensive ecosystem of which it is a part. Sometimes doing so is more manageable, such as through rigorously controlled and peer-reviewed experiments on the effects of digital experiences on human cognition and behaviour. It is from studies such as these that we are beginning to understand some of the addictive qualities of our digital experiences (which may help explain the panic you feel when you lose your device). But higher-level effects — e.g., the impact of social media on political polarization or authoritarianism — are far more difficult to untangle from other "confounding variables" (to use the language of social science). Societies are complex, and monocausal theories about them are almost always incorrect. Some of the effects people may attribute to social media — e.g., decline of trust in public institutions — are almost certainly the result of multiple, overlapping factors, some of which reach back decades. Attributing causality at a massive scale is always tricky for that reason.

One way I like to think about causal relationships at scale is to borrow from theories of biological evolution and describe social media as "environments" within which certain social forces flourish and multiply, or are constrained and wither. Framing causality this way avoids attributing specific effects solely to social media—what scientists sometimes refer to as "reductionism." The relationship between species and the environment of which they are a part is most pronounced when the environment suddenly changes, as with a volcanic eruption or asteroid collision. (Sixty-six million years ago, a ten-to-fifteen-kilometre-wide asteroid slammed into Earth, causing widespread climatic and other changes to the environment, leading to the extinction of roughly three-quarters of Earth's species.) Much as a sudden change in the natural environment can alter conditions in ways that favour some species over others, so too does our changing communications environment favour certain practices, ideas, and institutions over others (both positively and negatively). Seen through this lens, social media do not *generate* practices, ideas, and institutions *de novo*. The spread of disinformation in the public realm is not something Facebook or Twitter alone is responsible for. The practice of deliberately spreading false information is as old as humanity itself. However, social media's algorithms create conditions ripe for its propagation today, and as a consequence, disinformation practices are proliferating, becoming more elaborate, backed up with more resources, and thus potentially have more damaging effects than would be the case in the absence of social media.

Thinking about changing modes of communication as environments has a long pedigree, and a uniquely Canadian connection to boot. Many Canadians may not be aware of our country's important legacy around the study of communications technologies associated with the Toronto School of Communications, and in particular with University of Toronto alumni Harold Innis and Marshall McLuhan. (This family of theorizing is also known as "media ecology," and adherents of it have formed a large professional network called the Media Ecology Association.) Innis and McLuhan both drew attention in their different ways to the material qualities of different modes of communication and how these material qualities affect the nature and quality of communications. McLuhan was fond of speaking in aphorisms, and one of his most famous, "the medium is the message," was intended to encapsulate this thesis: the material properties of any particular communications technology affect the nature and character of the content of communications. Hence societies in which one particular mode of communication is predominant — the oral culture of ancient Greece or the print-based culture of early modern Europe — exhibit characteristics associated with those modes.

Innis, McLuhan, and other media ecologists have drawn attention to how the effects of modes of communication are pronounced in periods of rapid technological change, and in particular when societies transition from one mode of communication to another. The role of chance, or contingency, in human affairs has also been a prominent feature of media ecology, and in particular of the writings of Harold Innis. While human practices congeal and remain stable over long periods of time, making them feel like permanent fixtures (think of sovereign states as an example), they are nonetheless products of history and thus subject to change as nature, technology, and society evolve. In his seminal book *Empire and Communications*, Innis explained how several contingent social, political, technological, and environmental factors all combined to create circumstances advantageous to the rise of the Roman Catholic Church in the early Middle Ages:

> The spread of Mohammedanism cut off exports of papyrus to the east and to the west... Papyrus was produced in a restricted area and met the demands of a centralized administration whereas parchment as the product of an agricultural economy was suited to a decentralized system. The durability of parchment and the convenience of the codex for reference made it particularly suitable for the large books typical of scriptures and legal works. In turn, the difficulties of copying a large book limited the numbers produced. Small libraries

> with a small number of books could be established over large areas. Since the material of a civilization dominated by the papyrus roll had to be recopied into the parchment codex, a thorough system of censorship was involved. Pagan writing was neglected and Christian writing emphasized.

A different set of contingencies later connected to the development of mechanized printing (a wooden block form of which was first invented in eighth-century China and then adapted and improved upon in Europe in the fifteenth century by goldsmith Johannes Gutenberg) led in turn to the demise of the Roman Catholic Church's authority throughout Western Europe (despite that Gutenberg saw the Church as an important early client and sponsor). The invention of mass mechanized printing has also been connected to the rise of individualism (thanks to the silent reading it encouraged) and nationalism (thanks to standardized printed newspapers in vernacular languages), among other social effects.

The purpose of this section is not to simply detour into the history of communications for its own sake, but to remind us of the power of unintended consequences. Technologies designed for one purpose often end up having far-reaching impacts much different than what their designers envisioned. The same holds true not only for social media but for our entire communications ecosystem. Who knew that as social media climbed in popularity and more people acquired always-on mobile devices, these would prove to be a major source of insecurity exploited by autocrats and other bad actors? Who could have foreseen that a tool designed to forge bonds between communities would end up fostering social polarization and discord? Media ecologists remind us that changing technological environments can take human history in unexpected directions.

Media ecology had a major influence on my own intellectual outlook, and in particular on the establishment of the Citizen Lab, the research group I founded at the University of Toronto in 2001 and presently still direct. (My Ph.D. dissertation, which in 1997 became my first published book, titled *Parchment, Printing, and Hypermedia,* was an exploration of the implications for world order of changing modes of communication throughout history.) Innis's attention to material factors prompted me to examine more closely the often overlooked physical infrastructure of the internet — to dig beneath the surface of our communications ecosystem and uncover the exercise of power that goes on in subterranean realms. It is often said that everyone has at most one great idea, and if that's the case, mine was to recognize that there are powerful methods, tools, and techniques in computer and engineering sciences that could help uncover what's going on beneath the surface. Not being formally trained in these domains, I turned to others who were, and as a result the Citizen Lab was born, both interdisciplinary and collaborative from the start.

A colleague of mine once described what we do as a kind of "MRI of the internet," which captures the ways network scanning, reverse engineering, and other computer and engineering science techniques peel back the layers of our communications ecosystem. But I have also been inspired by other, more direct analogies. Since graduate school, I have been fascinated by the way government security agencies have for decades manoeuvred through the communications ecosystem largely outside of public view, thanks to classification and secrecy. Early in my career I became familiar with signals and other electronic intelligence gathering, and was quite shocked to discover how some states had secretly developed sophisticated means and elaborate tools to intercept and monitor telecommunications and other network traffic. The U.S. National Security Agency (NSA) and its partners in the "Five Eyes" alliance (United Kingdom, Canada, New Zealand, and Australia) were doing so on a planetary scale. While marvelling at this capacity (and putting aside legal, ethical, and other reservations), I wondered why a variation of it, based on open-sourced public research, couldn't be developed and used to turn the tables on governments themselves: to "watch the watchers" and reveal the exercise of power going on beneath the surface of our communications environment. A mission was thus established for the Citizen Lab, and our interdisciplinary research came into focus: to serve as "counter-intelligence for global civil society."

There's an old saying that comes to mind, though: *careful what you wish for*. When we first began our work at the Citizen Lab, we had no basis upon which to claim we were undertaking "counter-intelligence" for anyone, let alone global civil society. But gradually the methods, tools, and techniques became more refined; talented personnel were drawn to the mission and the freedom to explore challenging puzzles, the solutions for which had real-world consequences. Important collaborations developed and the case studies accumulated. We found ourselves pulling back the curtain on unaccountable actions that some very powerful actors would rather we did not. Not surprisingly, those powerful actors did not just sit on their hands and do nothing, and we have found ourselves more than once in the crosshairs. *Consider it a mark of success*, we've been told, and I tend to agree. Close to two decades of research, undertaken in collaboration with some enormously talented researchers, has helped inform my perspective on everything reported on in this book. Thanks to the work of the Citizen Lab, I feel as though I've been watching dark clouds forming on the horizon, and I along with my colleagues have been trying to raise the alarm that this is not a good sign.

A MAJOR AIM OF *RESET* is to help get us started thinking about how best to mitigate the harms of social media, and in doing so construct a viable communications ecosystem that supports civil society and contributes to the betterment of the human condition (instead of the opposite). It's clichéd to say that the time in which one lives is a "turning point." But looking around at the massive disruption to humanity's entire operating system, it is no exaggeration to say that we are in the midst of one. Even before the COVID-19 pandemic hit, many existing institutions and assumptions were already under the microscope. So too is the case for social media. In order to move forward positively, we need to have a clear understanding of the nature of the problems in the first place. The first four chapters of *Reset* lay out what I see as the principal "painful truths" about social media and, by extension, the entire technological landscape of which they are a part.

"It's the economy, stupid," political strategist James Carville once remarked, and it's a good reminder of where to begin to understand the pathologies of social media. Chapter 1 explores the economic engine that underlies social media: the personal data surveillance economy, or what Zuboff calls "surveillance capitalism" (a phrase actually first coined in 2014 by the Canada-based sociologist Vincent Mosco). Social media platforms describe themselves in many different, seemingly benign ways: "wiring the world," "connecting friends and family members," "all the world's information at your fingertips," and so on. And on the surface, they often live up to the billing. But regardless of how they present themselves, social media have one fundamental aim: to monitor, archive, analyze, and market as much personal information as they can from those who use their platforms. Constituted on the basis of surveillance capitalism, social media are relentless machines that dig deeper and deeper into our personal lives, attaching more and more sensors to more and more things, in a never-ending quest for unattainable omniscience. Over the course of the past two decades, they have done so spectacularly, accomplishing a degree of intimacy with average people's routines that is unprecedented in human history and flipping the relationship between user and platform. On the surface, it may seem like they're serving us (their customers) something useful and fun, but deeper down we have become their raw material, something akin to unwitting livestock for their massive data farms.

Chapter 2 examines the interplay between social media and social psychology. The job of social media engineers is to design their products in such a way as to capture and retain users' interests. In order to do so, they draw on insights and methods from commercial advertising and behavioural psychology, and they refine their services' features to tap into instincts and cognitive traits related to emotional and other reflexes. This dynamic means that social media's algorithms tend to surface and privilege extreme and sensational content, which in turn degrades the overall quality of discourse on the platforms. (How often have you heard someone remark that Twitter is a "toxic mess"?) It also creates opportunities for malicious actors to deliberately pollute social media and use them as channels to sow division, spread disinformation, and undermine cohesion. This appetite for subversion has even become big business as "dark" PR companies sell disinformation services to a wide range of clients. Although many factors have contributed to the recent descent into tribalism and social polarization, there can be no doubt the environment of social media has created conditions favourable for their flourishing.

Chapter 3 broadens out and scrutinizes the ways in which social media and other related digital technologies have contributed to what I call a "great leap forward in technologies of remote control." In a very short period of time, digital technologies have provided state security agencies with unparalleled capabilities to peer inside our lives, both at a mass scale and down to the atomic level. Part of the reason is the booming surveillance industry, which crosses over relatively seamlessly between private-sector and government clients, and has equipped security agencies with a whole new palette of tools they never previously could have imagined. But part of it is because the social media platforms upon which civil society relies are replete with insecurities. For most people, these insecurities create risks of fraud and other forms of personal data exploitation. For high-risk users, these insecurities can be life-threatening. This great leap forward in the technologies of remote control has taken place mostly in the shadows and in the absence of any compensating measures to prevent abuse. We now have twenty-first-century superpower policing governed by twentieth-century safeguards. As a consequence, already existing authoritarian regimes are tending towards a dystopian system of big-data population control, as exemplified in China's Orwellian "social credit system." Meanwhile, liberal democracies are exhibiting disturbing patterns of unaccountable policing and security practices that challenge existing safeguards against abuse of power. The COVID pandemic heightened these risks as governments declared emergency measures and turned to social media's vast machinery of personal data monitoring for purposes of biomedical surveillance.

Chapter 4 turns to the often overlooked and largely obscured physical and material infrastructure of social media and the communications ecosystem. Although we tend to think of social media and our digital experiences as clean, weightless, and ethereal (an image promoted by the platforms themselves), they are in fact far from it. Every component of our communications ecosystem is implicated in a vast, planet-wide physical and material infrastructure, the raw material for which can be traced back billions of years. Social media are not only inextricably connected to the natural world, they tax it in multiple surprising ways across a spectrum that includes mining, manufacturing, transportation, energy consumption, and waste. Although we often look to digital technologies as sustainability solutions, another painful truth about social media (at least as presently constituted) is that they are increasingly contributing to widespread environmental degradation.

Taken on its own, each of these painful truths is disturbing. When they are added up, they present a very bleak picture of our social and political reality, and an even bleaker forecast of our collective future. In combination, they can feel profoundly overwhelming, like a tectonic force that cannot be reversed. In part, that is why these truths are "painful." Examining each of their pathologies completely and unreservedly, understanding and appreciating their scope and scale, can leave one feeling exhausted and resigned. Perhaps that is why social media continue to grow in popularity in spite of the "techlash." Perhaps this explains why so many of us choose to remain in a state of blissful ignorance, never untethered for too long from our precious devices. But, as with the challenges of the climate crisis, fateful resignation to social media's disorders will only invite looming disaster. While the personal, social, political, and ecological implications of social media are profoundly disturbing, not doing anything to mitigate them will be far worse.

In the final chapter, I turn to the question "What is to be done?" The negative implications of social media are increasingly acknowledged and well documented. But what to do about them is a different matter. That's not to say that there are no proposed solutions. Indeed, those are abundant and multiplying, but they also lack an overarching framework that ties them together, and in some instances they are even contradictory. In the interests of pulling some of these partial solutions together, I make a plea for a single, overarching principle to guide us moving forward: *restraint*. The common-sense meaning of "restraint" is keeping someone or something under control, including our emotions, our habits, and our behaviours.

What may be less apparent to many readers is that restraint, while seemingly simple, is a concept with a rich historical legacy connected to a long line of political thinking and practice that reaches all the way back to ancient Greece. Restraints are at the heart of liberal political theory, and more specifically that family of liberal theorizing known as "republicanism," derived from the Latin *res publica* (and not to be confused with the party that goes by that name in the United States). Republican thinkers from Polybius to Publius and beyond have seen restraints as critical to checking the state to prevent abuse of power. Police put restraints on criminals, and we, in turn, put restraints on police. Restraints of the latter sort are sorely missing in some areas of life, and rapidly threatened by technological change in others. Drawing inspiration from some of the ways republican-inspired thinkers have conceptualized restraint mechanisms in the past, I put forward some suggestions for how we might think about restraint measures in our own times — as means to rein in the excesses of social media and guard against abuses of power, all the while preserving the great potential of our communications ecosystem. After our reset, I argue, we need to double down on *restraint*.

WHILE *RESET* IS WRITTEN in the context of the COVID-19 pandemic, its larger backdrop is the looming climate crisis and the existential risks it poses to human civilization. As environmental activist and author Naomi Klein has put it, "Humbling as it may be, our shared climate is the frame inside which all of our lives, causes, and struggles unfold." If it wasn't apparent before, it should be now: nature is an inescapable force and the foundation for our very being. Pandemics, rising sea levels, melting ice caps, and escalating surface temperatures show that we are all in this together: one species, one planet.

The many different applications that make up our communications ecosystem will be integral to environmental rescue and ensuring the continued habitability of planet Earth. The internet and even social media hold out the promise of peer-to-peer communications on a global scale, essential for sharing ideas and debating our collective future. The myriad of sensors that span the globe, from satellites in near-Earth orbital space down to biomedical sensors implanted in our bodies, will be essential to taking the pulse of the planet's vast ecology, our own habitat included. Machine-based calculations undertaken at quantum scale can help us solve complex puzzles, increase efficiencies, and help predict and weigh the benefits of alternative trajectories.

However, the time has come to recognize that our communications ecosystem — as presently constituted around surveillance capitalism — has become entirely dysfunctional for those aims. It's disrupting institutions and practices and unleashing new social forces in unexpected ways, many of which are having malign effects. Emergency measures now in place could turn superpower policing practices into totalitarian-scale population controls that quash individual liberties while creating unbridled opportunities for corruption and despotism. Runaway technological innovation for its own sake continues on a disastrous path of unbridled industrial consumption and waste, obscured by the mirage of virtuality. Leaving it as is, with all of its intertwined pathologies intact, will all but ensure failure. A reset gives us a rare opportunity to imagine an alternative, and begin the process of actually bringing it about. To be sure, it won't be easy, nor will it happen overnight. But fatalistic resignation to the status quo is no real alternative either.