Introduction
Careering Down a Road Hardly Anyone Wants to Take

It’s hard to find anyone willing to predict a bright future for privacy in America. Some simply claim indifference to the fate of what they decry as an anachronistic value. But many are quietly alarmed to see us speeding headlong down a road that few really want to take, but which no one seems able to quit. At the end of this road lies a world where all our recorded information flows seamlessly from one interested party to the next—regardless of our wishes. Few of us, I believe, welcome this trajectory.

Propelling us in this direction are the ingenious and precisely targeted efforts of organizations—resourceful government agencies and corporate bureaucracies whose place in the sun depends on what they can do with our data. These parties make it their specialty to master the details of our pasts in order to orchestrate our futures. Sometimes we experience their attentions as uncomfortable, unilateral impositions—as when tax authorities demand documentation for obscure details of our lives, with threat of penalties if we balk. Elsewhere, we uneasily find ourselves complicit in undoing our own privacy, while downloading smartphone apps, installing communications software, or logging on to social media. As we click through opaquely written privacy notices, terms of service, and user agreements, we sense—often correctly—that we are yielding much more
than we know. Strictly speaking, we may have the option to step back—to renounce the connection or the service at hand. But since the activities in question are increasingly defined as part of normal life, few choose to turn away.

Even those of us determined to guard access to our personal data find that resistance doesn’t get us very far. We live in a world organized unobtrusively to extract and record pertinent information about our whereabouts, our states of mind, our consumer choices, and our political attitudes without our consent—and often without our knowledge. The prescriptions we order, the topics and timing of our phone and email communications, the parties we communicate with; details of our domestic and international travels; even our choices of X-rated videos—these are just a few of an enormously long and constantly growing list of crucial personal data that we shed. Any and all of these fragments of our biographies are subject to being sold, traded, or otherwise directed to government and private organizations dedicated to using them to shape their treatment of us. The fact that we cannot censor information about ourselves collected in these ways makes it especially valuable to organizations seeking it. For such unguarded disclosures are apt to afford the most telling insights into what we’re apt to do—or think or want—next.

Countless organizations on which we rely to get on with our lives crave to know things about us that we may not care to share. Credit grantors take an interest precisely in those past accounts where our payment patterns have been spotty or worse. Insurance companies prefer to sell coverage to customers who never even think about making a claim—let alone those with a history of doing so. The Internal Revenue Service wants to know about windfall income and well-paid special assignments that taxpayers are least likely to volunteer on their returns. Such tensions, and countless others like them, have been with us far longer than computing. What information technologies have added is the possibility of recording—and sharing,
analyzing, cross-checking, slicing, and dicing—the fine details of our daily lives in ways that reveal what would otherwise remain obscure. What’s more, realizing the rich payoffs that ensue from cross-referencing self-generated information about us to that derived from outside sources, organizations develop *algorithms* that point to connections any one investigator is unlikely to make on her own.

As law professor Frank Pasquale points out, one never knows when some imaginative combination of personal data may start ringing alarm bells where they’re least expected. He offers as an example “the plight of Walter and Paula Shelton, a Louisiana couple who sought health insurance. Humana, a large insurer based in Kentucky, refused to insure them based on Paula’s prescription history—occasional use of an antidepressant as a sleep aid and a blood pressure medication to relieve swelling in her ankles. The Sheltons couldn’t get insurance from other carriers, either. How were they to know that a few prescriptions could render them pariahs? . . . But since then, prescription reporting has become big business: one service claimed reports of ‘financial returns of 5:1, 10:1, even 20:1’ for its clients.” The author notes that the Affordable Care Act may now shield the couple from discrimination like that described here, through its protections for patients with preexisting conditions. Chapter 2 of this book explains more fully how data on their prescriptions captured from this couple’s pharmacists may have tipped insurance companies to avoid them.

The drip-drip-drip accumulation of personal information resulting from such connections may pass without notice in a world where computer monitoring of our actions has become a daily, if not hourly, experience. Still less obvious is the growing power of those who control the systems—from social media to government watch lists to marketing databases—as they broaden in their coverage, and fuse with one another in ever-new combinations and symbioses.

Such emerging forces in American life are not simply manifestations of technology. These phenomena are *political* both in their
inspiration and in their consequences. Changes in who-can-know-what-about-whom inevitably bring transformations in power and authority. Taxation, for example, is always dependent on availability of information on the people and things to be taxed. And it avails the authorities little to declare a levy on consumption of internet pornography, for another example, unless means exist to identify and track such content. Such surveillance, though, is by no means beyond the capabilities of current technologies. Is America ready to accept a “sin tax” on porn—to go with extra charges levied against tobacco and alcoholic drinks?

And have Americans fully come to terms with the possibilities of using—or abusing—such surveillance capacities to distort basic processes of democracy? Nearly everyone remembers the revelations of attempted misuse of personal data in the 2016 presidential election: Cambridge Analytica, a shadowy British company, obtained data on millions of Facebook members, with the intent of manipulating their votes in the presidential election.

Attempts to distort expressions of opinion between the public and government by no means ceased with those events. In an effort to inform its expected ruling on net neutrality, the Federal Communications Commission opened its website to public comments. According to an account from April 2018, it received more than twenty-two million comments. But close investigation of such efforts to canvass public sentiment on major policy issues has documented stunning efforts to manipulate the results. The Wall Street Journal, for example, dug into the backstory behind a Labor Department forum involving public views for and against changes in the “fiduciary rule” requiring retirement advisors to act in the best interests of their clients. A difficult principle to oppose, one might have thought. But the WSJ analysis of the “public comments” on the proposed changes found that some 40 percent of them were fake—posted under the names of real people, but not by those who allegedly authored them.
Many of these false public voices appeared to be impersonations of those whose identities had been compromised by at least one data breach.²

· · ·

Many of these possibilities for deception and manipulation remain largely unknown, even to those with long experience in these matters. *Washington Post* writer Geoffrey Fowler has published an in-depth inquiry into the “fingerprinting” of computers—techniques by which organizations can determine the identities of parties they are interacting with—even when the latter take all available measures to cover their electronic tracks. Their computers can force yours, Fowler reports, to give up information on matters like the resolution of your screen, your operating system, and the fonts you’re using—technical details, perhaps, but distinctive enough in the ensemble to reveal your identity. “At least a third of the 500 sites Americans visit most often use hidden code to run an identity check on your computer at home,” he concludes.³ Thus, companies devoted to providing pornography over the internet may know your preferences in this form of entertainment before you even log on—inductively, one might say, simply by generalizing your taste in this medium as manifested across many visits.

Yet such subtle invasions of privacy pale in comparison to what today’s personal-data systems could do, if mobilized under an overtly repressive regime. They could track the whereabouts of political dissenters, for example, or disable their bank accounts, or pressure their friends. A regime with totalitarian intent, abetted by present-day technologies and management techniques for manipulating personal data, would create a “perfect storm” for democratic institutions. Without strong legal and policy checks against such uses, we could find ourselves approaching authoritarian rule through the back
door—developing an arsenal for intrusive scrutiny over once-private areas of life that would go unnoticed until used for the most destructive purposes.

American law has never developed a unified philosophy of privacy. This is scarcely to say that we have no significant protections for personal information, but rather that restrictions on what can be learned about and done with personal data derive from disparate sources—some from the Constitution, some from tort law, some from criminal law. Fourth Amendment constitutional protections against state powers to obtain certain personal records block some forms of intrusion into people’s homes. But the fact that so much personal data is stored outside Americans’ homes—in banks, credit card account records, and the like—greatly reduces the overall significance of the Fourth Amendment as a source of privacy protection muscle.

The closest this country comes to European-style privacy legislation grounded in a clearly defined “right to privacy” and applying a single set of principles to an open-ended variety of cases is the Privacy Act of 1974. This key statute governs treatment of personal data held by U.S. government agencies. In the underlying principles it invokes, it hearkens directly to the influential publication *Records, Computers, and the Rights of Citizens* (1973)—the source of the much-noted Fair Information Practices that have since influenced so much legislation and policy throughout the world (see this book’s preface).

Here and elsewhere, the rise of large-scale personal-data systems designed to guide government or corporate action toward “private” citizens has fostered a new *genre* of jurisprudence. Since the 1970s, legislators and policymakers both in this country and abroad have sought to constrain the use of personal information in the face of these new modes of action. These efforts have resulted in the
proliferation of national privacy codes—now more widely termed “personal data protection” laws to an estimated more than two hundred countries outside the United States. First in Northern and Western Europe, then increasingly throughout the globe, these bodies of law have come to shape practice both in government and in the private sector.

But America’s privacy codes have afforded little defense against the salient privacy setbacks of the last generation—the rise of industries devoted to compiling and retailing Americans’ personal information, for example; or the intrusive monitoring of telecommunications metadata by shadowy government agencies; or the rise of social media, with their weak privacy guarantees and their determination to market insights into personal attitudes and susceptibilities that we may not be aware of ourselves.

We can do much better. America’s efforts to protect privacy in the face of encroaching demands for personal information have not matched the enormity of the forces that they are supposed to address. Indeed, American legislation and policy have often approached these issues on the basis of potentially disastrous assumptions. One is that any existing system of accounting and tracking of individuals’ lives—government or private—must correspond to some authentic, shared social need. In this view, the reformers’ task becomes one of adding privacy to existing practices, without threatening the key performances of the organizations involved. The resulting measures may indeed succeed in granting the subjects of the recordkeeping some significant relief. But they leave the most historic and consequential questions unanswered. Above all, how much and what forms of such human tracking deserve a place in a liberal and democratic social order in the first place? And what can we do to reduce the extreme asymmetries in options for action between data-holding organizations and grassroots citizens and consumers? In other words, what steps can we take to make Americans
not just subjects of institutional recordkeeping, but instead active and effective agents of their own privacy interests?

This book takes such questions as its point of departure. It seeks to break with a tradition of American privacy protection that, for all its virtues, has proved excessively reactive to the ever-emergent stream of privacy outrages. Instead of asking how we might somehow add privacy constraints to existing personal-data systems, I want to pose what strike me as prior questions. In the best of possible worlds, what uses of recorded personal information would serve us most efficiently? What legal and policy principles would someone who takes privacy seriously want to uphold—and what practices should simply be abandoned?

How can we define privacy for the purposes of this book? This usefully vague term refers to a mixed array of human interests that are clearly akin to one another, yet distinct. One of these is a felt need for autonomy in decision-making and action—the insistence on respect for realms where one makes up one’s own mind and charts one’s own course of action. People often assert this form of privacy interest in matters of birth control and abortion. Here as elsewhere, an interest in keeping certain knowledge to oneself stems from broader desires not to have to account to anyone else for crucial decisions. So, the ruling in the famous court case Griswold v. Connecticut—that the state could not ban the use of contraceptives by married people—is characterized as a victory for marital privacy, in this sense of autonomy.

Another basic human desire often understood as a privacy interest is the wish to avoid embarrassing exposure. Hardly anyone likes the prospect of being forced to disrobe when all others present are clothed, or being spied upon when assuming that one is alone. We
have similar desires to avoid publication of details of medical treatments that we find awkward, or public review (in court proceedings, for example) of incidents that we consider shameful or embarrassing. The law, in many states, recognizes this privacy interest—as in statutes prohibiting publication of the names of rape victims or dissemination of revenge pornography.

Information privacy, people’s interests in institutional compilation and use of data held in file about themselves, has attracted the lion’s share of commentary over the past five decades—no surprise, given the skyrocketing growth in personal-data systems and their consequences for the lives of those depicted in them. Nearly everyone today takes it for granted that their “records” follow them through life, with weighty results—even if one is unable to specify fully what those records consist of, or precisely to detail their uses. Information privacy—often shading off into these related forms—is the main focus of this book.

Keeping these distinct meanings of privacy in mind wins us a measure of precision. But I nevertheless believe that our use of the vague but inclusive term privacy, with its multiple, overlapping meanings and connotations, has value of its own. We need to think of privacy as what philosopher W. B. Gallie called an “essentially contested concept”—an idea destined to be argued over and reassessed as long as issues of autonomy, exposure, and treatment of recorded information matter in human affairs. As with “liberty,” “justice,” “good citizenship,” or “democracy,” understandings of privacy inevitably have a normative element, in that most people consider a certain measure of it, at least, a good thing. But if privacy in some sense is indeed desirable, then what policies and practices most effectively promote it—or promote the “right” kinds of privacy, or privacy in the right contexts? Most of us would not opt for granting unlimited privacy to former felons regarding their criminal histories, for example. So, how do we distinguish appropriate and indispensable forms of privacy
protection from those that would wreak undeserved hardship? These are classic questions raised by essentially contested concepts.

We can’t expect definitive settlement of such questions. Perhaps this is because every age and every intellectual constituency brings different concerns to the debate, so that what counts as a satisfactory understanding for one thinker at one moment will miss the mark for others. When we speak of privacy, we point to an inchoate complex of values and interests that is constantly undergoing redefinition and reinterpretation. Perhaps this is unsatisfying. But we can’t get along without essentially contested concepts—or at least, we shouldn’t want to—because struggling to define and apply them anew is essential to our efforts to make the best of the world we live in.

What do I mean, then, by “taking privacy seriously”? I mean, above all, placing privacy on a par with state security, institutional efficiency, and other social goods with which it inevitably competes. I mean being willing to renounce some—by no means all—of the securities and comforts afforded by today’s personal-information systems in the interests of privacy. I mean being prepared to run the risk of dialing down some—not all—of the intrusive surveillance measures that today fly under the flag of national security. And I mean being candid about the costs that must be paid for refusing to exploit every bit of personal information for institutional ends—for example, in giving some poor credit risks a “second chance” to borrow and repay, or allowing a former convict who has broken with his or her past to live quietly and without discovery.

This needs some unpacking. I hardly imagine that every reader of this book joins me in embracing all the privacy-friendly priorities cited above. Some will proceed from quite different assessments—for example, the notion that the world is so dangerous and disorderly
that intensified supervision and closer discipline of citizens’ lives is the only reasonable policy. Others might hold that privacy values are ultimately a matter of indifference to most people, most of the time, and hence do not warrant the significant costs needed to uphold them. Those readers will approach the following pages as a road map for a trip they do not wish to take.

What can I say to persuade those readers to share my view? I take it as axiomatic that differences of political vision like these are only partly susceptible to resolution through appeals to evidence—if by “evidence” one means empirically observable data. Often such conflicts in worldview more closely resemble differences of taste in art, recreational habits, or even food than disputes over matters of empirical fact. We can and must be prepared to argue for the workability of any values or tastes that we choose—that is, for their ability to direct and sustain a social world we would be prepared to live in. But we should never deceive ourselves that the role of such tastes can somehow be eliminated. Some citizens—not too many, I suspect, but some—simply feel little attachment to privacy values, at least as compared to competing values. The latter include strict adherence to social rules and rigorous defense of efficiency—from punishing welfare cheaters and tax evaders to making the trains run on time. But they, like we, must offer their fellow citizens some account of how their (or our) favored values could work in practice to animate a livable and attractive world.

Still, I believe that I am far from alone in embracing the key values guiding this work. Few of us are really comfortable contemplating a world where, like it or not, everyone generates more and more recorded personal information simply in the course of everyday living—and where any and all such information automatically becomes available to interested decision-makers elsewhere. Against that view, those of us willing to take measured risks on behalf of privacy need some sort of program of public action. In their necessarily
reactive role in decrying obvious privacy outrages, American privacy advocates have often missed opportunities to project positive, comprehensive statements of what they are for. What sort of world would we want to create, if we had full liberty to fashion institutions and practices with privacy as a central value?

The privacy values at issue are of two kinds. First are strictly individual goods implicated in the flow of personal information. These range from those at stake in dissemination of painful or embarrassing facts—as in disclosures from sensitive medical records, or in revenge pornography—to revelation of information that is strategically disadvantageous, as in release of genetic information that blocks access to employment. What these interests or values have in common is that they may be satisfied for one person, yet unfulfilled for the next—just as one may be well fed, for example, while one’s neighbors starve.

But a second kind of privacy value also requires our advocacy—those values that can only be experienced jointly, as part of some larger group. One cannot enjoy the satisfactions of nationalism, for example, without a nation to belong to. Or—as is often said—one cannot fully enjoy the virtues of freedom of expression, unless others do the same. A major payoff of such freedom, after all, should be the benefits derived from full exchange of ideas among one’s fellow citizens—something impossible if any group feels constrained against speaking out. Privacy is like that. The chilling effects generated by a conviction that large institutions know everything about us can be far-reaching, whether that belief is well founded or not. Accordingly, we all have an interest in each other’s privacy—in a social order where no one need fear oppressive snooping.

There is nothing contradictory about pursuing both these goals in a single program. Safeguards that we might desire for ourselves are equally valid when sought on behalf of our fellow citizens. Under prevailing American law, personal data are largely governed by what
might be called “finders-keepers” principles, at least with regard to commercial use. As the following chapters demonstrate, information ranging from the details of our internet searches to the prescriptions we order from the pharmacy are subject to opportunistic capture, reuse, and resale by organizations we trust to handle them, or those that pay such organizations for access to the data—hence Americans’ widespread, and largely justified, perception that control over one’s “own” data, once released, is permanently lost. The reforms proposed here seek to reverse this state of affairs. They even go so far as to propose (in chapter 6), a universal property right over commercialization of information on oneself, so that no such use would be possible without explicit consent from the subject.

Any attempt to enact such reform, needless to say, will trigger tectonic collisions of interest with the parties now controlling commercialization of our personal information. Simply injecting this possibility into public discussion would send an unmistakable message that today’s regime for the use of personal data is not the unique or inevitable consequence of prevailing technologies. It is exactly the sort of easily understood, politically potent possibility—like Medicare for all, or paid family leave, or a direct tax on carbon emissions—that could fuel a movement endowed with a positive social vision of a drastically more private world. The mere fact that such alternate realities can be acknowledged and discussed refutes one of the most dangerous anti-privacy themes of current culture—the notion that today’s privacy-challenged practice represents the only possible result of our reliance on computing technologies.

This book proposes eleven potent and easily grasped privacy-friendly principles, and seeks to weave them into a comprehensive vision. The scarcity of such visions, I hold, has undermined possibilities for a strong, grassroots movement on behalf of privacy in American life. Americans have heard so many times that they have “chosen” a more convenient, diverting, comfortable informational world