THE BLACK BOX SOCIETY

The Secret Algorithms That Control Money and Information

FRANK PASQUALE

Harvard University Press

Cambridge, Massachusetts
London, England
2015

1

INTRODUCTION—THE NEED TO KNOW

EVERYBODY KNOWS the story about the man crawling intently around a lamppost on a dark night. When a police officer comes along and wants to know what he's doing, he says he's looking for his keys. "You lost them here?" asks the cop. "No," the seeker replies, "but this is where the light is." This bromide about futility has lately taken on a whole new meaning as a metaphor for our increasingly enigmatic technologies.

There's a noble tradition among social scientists of trying to clarify how power works: who gets what, when, where, and why.[1] Our common life is explored in books like *The Achieving Society*, *The Winner-Take-All Society*, *The Good Society*, and *The Decent Society*. At their best, these works also tell us why such inquiry matters.[2]

But efforts like these are only as good as the information available. We cannot understand, or even investigate, a subject about which nothing is known. Amateur epistemologists have many names for this problem. "Unknown unknowns," "black swans," and "deep secrets" are popular catchphrases for our many areas of social blankness.[3] There is even an emerging field of "agnotology" that studies the "structural production of ignorance, its diverse causes and conformations, whether brought about by neglect, forgetfulness, myopia, extinction, secrecy, or suppression."[4]

Gaps in knowledge, putative and real, have powerful implications, as do the uses that are made of them. Alan Greenspan, once the most powerful central banker in the world, claimed that today's markets are driven by an "unredeemably opaque" version of Adam Smith's "invisible hand," and that no one (including regulators) can ever get "more than a glimpse at the internal workings of the simplest of modern financial systems." If this is true, libertarian policy would seem to be the only reasonable response. Friedrich von Hayek, a preeminent theorist of laissez-faire, called the "knowledge problem" an insuperable barrier to benevolent government interventions in the economy.[5]

But what if the "knowledge problem" is not an intrinsic aspect of the market, but rather is deliberately encouraged by certain businesses? What if financiers keep their doings opaque on purpose, precisely to avoid or to confound regulation? That would imply something very different about the merits of deregulation.

The challenge of the "knowledge problem" is just one example of a general truth: What we do and don't know about the social (as opposed to the natural) world is not inherent in its nature, but is itself a function of social constructs. Much of what we can find out about companies, governments, or even one another, is governed by law. Laws of privacy, trade secrecy, the so-called Freedom of Information Act—all set limits to inquiry. They rule certain investigations out of the question before they can even begin. We need to ask: To whose benefit?

Some of these laws are crucial to a decent society. No one wants to live in a world where the boss can tape our bathroom breaks. But the laws of information protect much more than personal privacy. They allow pharmaceutical firms to hide the dangers of a new drug behind veils of trade secrecy and banks to obscure tax liabilities behind shell corporations. And they are much too valuable to their beneficiaries to be relinquished readily.

Even our political and legal systems, the spaces of our common life that are supposed to be the most open and transparent, are being colonized by the logic of secrecy. The executive branch has been lobbying ever more forcefully for the right to enact and enforce "secret law" in its pursuit of the "war on terror," and voters contend in

an electoral arena flooded with "dark money"—dollars whose donors, and whose influence, will be disclosed only *after* the election, if at all.[6]

But while powerful businesses, financial institutions, and government agencies hide their actions behind nondisclosure agreements, "proprietary methods," and gag rules, our own lives are increasingly open books. Everything we do online is recorded; the only questions left are to whom the data will be available, and for how long. Anonymizing software may shield us for a little while, but who knows whether trying to hide isn't itself the ultimate red flag for watchful authorities? Surveillance cameras, data brokers, sensor networks, and "supercookies" record how fast we drive, what pills we take, what books we read, what websites we visit. The law, so aggressively protective of secrecy in the world of commerce, is increasingly silent when it comes to the privacy of persons.

That incongruity is the focus of this book. How has secrecy become so important to industries ranging from Wall Street to Silicon Valley? What are the social implications of the invisible practices that hide the way people and businesses are labeled and treated? How can the law be used to enact the best possible balance between privacy and openness? To answer these questions is to chart a path toward a more intelligible social order.

But first, we must fully understand the problem. The term "black box" is a useful metaphor for doing so, given its own dual meaning. It can refer to a recording device, like the data-monitoring systems in planes, trains, and cars. Or it can mean a system whose workings are mysterious; we can observe its inputs and outputs, but we cannot tell how one becomes the other. We face these two meanings daily: tracked ever more closely by firms and government, we have no clear idea of just how far much of this information can travel, how it is used, or its consequences.[7]

The Power of Secrecy

Knowledge is power. To scrutinize others while avoiding scrutiny oneself is one of the most important forms of power.[8] Firms seek out intimate details of potential customers' and employees' lives, but give regulators as little information as they possibly can about

their own statistics and procedures.[9] Internet companies collect more and more data on their users but fight regulations that would let those same users exercise some control over the resulting digital dossiers.

As technology advances, market pressures raise the stakes of the data game. Surveillance cameras become cheaper every year; sensors are embedded in more places.[10] Cell phones track our movements; programs log our keystrokes. New hardware and new software promise to make "quantified selves" of all of us, whether we like it or not.[11] The resulting information—a vast amount of data that until recently went unrecorded—is fed into databases and assembled into profiles of unprecedented depth and specificity.

But to what ends, and to whose? The decline in personal privacy might be worthwhile if it were matched by comparable levels of transparency from corporations and government. But for the most part it is not. Credit raters, search engines, major banks, and the TSA take in data about us and convert it into scores, rankings, risk calculations, and watch lists with vitally important consequences. But the proprietary algorithms by which they do so are immune from scrutiny, except on the rare occasions when a whistleblower litigates or leaks.

Sometimes secrecy is warranted. We don't want terrorists to be able to evade detection because they know exactly what Homeland Security agents are looking out for.[12] But when every move we make is subject to inspection by entities whose procedures and personnel are exempt from even remotely similar treatment, the promise of democracy and free markets rings hollow. Secrecy is approaching critical mass, and we are in the dark about crucial decisions. Greater openness is imperative.

Reputation, Search, Finance

At the core of the information economy are Internet and finance companies that accumulate vast amounts of digital data, and with it intimate details of their customers'—our—lives. They use it to make important decisions about us and to influence the decisions we make for ourselves. But what do we know about them*?* A bad credit score may cost a borrower hundreds of thousands of dollars, but he will never understand exactly how it was calculated. A predictive

analytics firm may score someone as a "high cost" or "unreliable" worker, yet never tell her about the decision.

More benignly, perhaps, these companies influence the choices we make ourselves. Recommendation engines at Amazon and YouTube affect an automated familiarity, gently suggesting offerings they think we'll like. But don't discount the significance of that "perhaps." The economic, political, and cultural agendas behind their suggestions are hard to unravel. As middlemen, they specialize in shifting alliances, sometimes advancing the interests of customers, sometimes suppliers: all to orchestrate an online world that maximizes their own profits.

Financial institutions exert direct power over us, deciding the terms of credit and debt. Yet they too shroud key deals in impenetrable layers of complexity. In 2008, when secret goings-on in the money world provoked a crisis of trust that brought the banking system to the brink of collapse, the Federal Reserve intervened to stabilize things—and kept key terms of those interventions secret as well. Journalists didn't uncover the massive scope of its interventions until late 2011.[13] That was well after landmark financial reform legislation had been debated and passed—*without* informed input from the electorate—and then watered down by the same corporate titans whom the Fed had just had to bail out.

Reputation. Search. Finance. These are the areas in which Big Data looms largest in our lives. But too often it looms invisibly, undermining the openness of our society and the fairness of our markets. Consider just a few of the issues raised by the new technologies of ranking and evaluation:

- Should a credit card company be entitled to raise a couple's interest rate if they seek marriage counseling? If so, should cardholders know this?
- Should Google, Apple, Twitter, or Facebook be able to shut out websites or books entirely, even when their content is completely legal? And if they do, should they tell us?
- Should the Federal Reserve be allowed to print unknown sums of money to save banks from their own scandalous behavior? If so, how and when should citizens get to learn what's going on?

- Should the hundreds of thousands of American citizens placed on secret "watch lists" be so informed, and should they be given the chance to clear their names?

The leading firms of Wall Street and Silicon Valley are not alone in the secretiveness of their operations, but I will be focusing primarily on them because of their unique roles in society. While accounting for "less than 10% of the value added" in the U.S. economy in the fourth quarter of 2010, the finance sector took 29 percent—$57.7 billion—of profits.[14] Silicon Valley firms are also remarkably profitable, and powerful.[15] What finance firms do with money, leading Internet companies do with attention. They direct it toward some ideas, goods, and services, and away from others. They organize the world for us, and we have been quick to welcome this data-driven convenience. But we need to be honest about its costs.

Secrecy and Complexity

Deconstructing the black boxes of Big Data isn't easy. Even if they were willing to expose their methods to the public, the modern Internet and banking sectors pose tough challenges to our understanding of those methods. The conclusions they come to—about the productivity of employees, or the relevance of websites, or the attractiveness of investments—are determined by complex formulas devised by legions of engineers and guarded by a phalanx of lawyers.

In this book, we will be exploring three critical strategies for keeping black boxes closed: "real" secrecy, legal secrecy, and obfuscation. *Real secrecy* establishes a barrier between hidden content and unauthorized access to it. We use real secrecy daily when we lock our doors or protect our e-mail with passwords. *Legal secrecy* obliges those privy to certain information to keep it secret; a bank employee is obliged both by statutory authority and by terms of employment not to reveal customers' balances to his buddies.[16] *Obfuscation* involves deliberate attempts at concealment when secrecy has been compromised. For example, a firm might respond to a request for information by delivering 30 million pages of documents, forcing its investigator to waste time looking for a needle in a haystack.[17] And

the end result of both types of secrecy, and obfuscation, is *opacity*, my blanket term for remediable incomprehensibility.[18]

Detailed investment prospectuses, for instance, can run to dozens or hundreds of pages. They can refer to other documents, and those to still others. There may be conflicts among the documents that the original source references.[19] Anyone really trying to understand the investment is likely to have to process thousands of pages of complicated legal verbiage—some of which can be quite obfuscatory. The same holds for accounting statements. When law professor Frank Partnoy and Pulitzer Prize–winning journalist Jesse Eisinger teamed up to explore "what's inside America's banks" in early 2013, they were aghast at the enduring opacity. They reported on the banks as "'black boxes' that may still be concealing enormous risks—the sort that could again take down the economy."[20] Several quotes in the article portrayed an American banking system still out of control five years after the crisis:

- "There is no major financial institution today whose financial statements provide a meaningful clue" about its risks, said one hedge fund manager.
- "After serving on the [Financial Accounting Standards] board [FASB]," said Don Young, "I no longer trust bank accounting."
- Another former FASB member, asked if he trusted bank accounting, answered: "Absolutely not."[21]

These quotes came five years after the financial crisis and three years after the Dodd-Frank Act, a gargantuan piece of legislation that comprehensively altered banking law. Financial crises result when a critical mass of investors act on that distrust, and their skepticism cascades throughout the system. And when governments step in with their "bailouts" and "liquidity facilities," they add new layers of complexity to an already byzantine situation.

In the case of technology companies, complexity is not as important as secrecy. However sprawling the web becomes, Google's search engineers are at least working on a "closed system"; their own company's copies of the Internet. Similarly, those in charge of Twitter and Facebook "feeds" have a set body of information to

work with. Their methods are hard to understand primarily because of a mix of real and legal secrecy, and their scale. Interlocking technical and legal prohibitions prevent anyone outside such a company from understanding fundamental facts about it.

Activists often press for transparency as a solution to the black box issues raised in this book. In many cases, sunshine truly is the "best disinfectant." However, transparency may simply provoke complexity that is as effective at defeating understanding as real or legal secrecy. Government has frequently stepped in to require disclosure and "plain language" formats for consumers. But financiers have parried transparency rules with more complex transactions. When this happens, without substantial gains in efficiency, regulators should step in and limit complexity. Transparency is not just an end in itself, but an interim step on the road to intelligibility.

The Secret Judgments of Software

So why does this all matter? It matters because authority is increasingly expressed algorithmically.[22] Decisions that used to be based on human reflection are now made automatically. Software encodes thousands of rules and instructions computed in a fraction of a second. Such automated processes have long guided our planes, run the physical backbone of the Internet, and interpreted our GPSes. In short, they improve the quality of our daily lives in ways both noticeable and not.

But where do we call a halt? Similar protocols also influence—invisibly—not only the route we take to a new restaurant, but which restaurant Google, Yelp, OpenTable, or Siri recommends to us. They might help us find reviews of the car we drive. Yet choosing a car, or even a restaurant, is not as straightforward as optimizing an engine or routing a drive. Does the recommendation engine take into account, say, whether the restaurant or car company gives its workers health benefits or maternity leave? Could we prompt it to do so? In their race for the most profitable methods of mapping social reality, the data scientists of Silicon Valley and Wall Street tend to treat recommendations as purely technical problems. The values and prerogatives that the encoded rules enact are hidden within black boxes.[23]

The most obvious question is: Are these algorithmic applications fair? Why, for instance, does YouTube (owned by Google) so consistently beat out other video sites in Google's video search results? How does one particular restaurant or auto stock make it to the top of the hit list while another does not? What does it mean when Internet retailers quote different prices for the same product to different buyers? Why are some borrowers cut slack for a late payment, while others are not?

Defenders of the status quo say that results like these reflect a company's good-faith judgment about the quality of a website, an investment, or a customer. Detractors contend that they cloak self-serving appraisals and conflicts of interest in a veil of technological wizardry. Who is right? It's anyone's guess, as long as the algorithms involved are kept secret. Without knowing what Google actually *does* when it ranks sites, we cannot assess when it is acting in good faith to help users, and when it is biasing results to favor its own commercial interests. The same goes for status updates on Facebook, trending topics on Twitter, and even network management practices at telephone and cable companies. All these are protected by laws of secrecy and technologies of obfuscation.

The One-Way Mirror

With so much secrecy so publicly in place, it is easy for casual observers to conclude that there is a rough parity between the informational protection of individuals and civil associations and those of corporations and government. It is comforting to think that our personal bank records are as secure as the bank's own secrets. But I will attempt to overthrow this assumption. We do not live in a peaceable kingdom of private walled gardens; the contemporary world more closely resembles a one-way mirror. Important corporate actors have unprecedented knowledge of the minutiae of our daily lives, while we know little to nothing about how they use this knowledge to influence the important decisions that we—and they—make.

Furthermore, even as critical power over money and new media rapidly concentrates in a handful of private companies, we remain largely ignorant of critical ways in which these companies interact

(and conflict) with public powers. Though this book is primarily about the private sector, I have called it *The Black Box Society* (rather than *The Black Box Economy*) because the distinction between state and market is fading. We are increasingly ruled by what former political insider Jeff Connaughton called "The Blob," a shadowy network of actors who mobilize money and media for private gain, whether acting officially on behalf of business or of government.[24] In one policy area (or industry) after another, these insiders decide the distribution of society's benefits (like low-interest credit or secure employment) and burdens (like audits, wiretaps, and precarity).

Admittedly, as Jon Elster has written in his book *Local Justice*, there is no perfectly fair way to allocate opportunities.[25] But a market-state increasingly dedicated to the advantages of speed and stealth crowds out even the most basic efforts to make these choices fairer. Technocrats and managers cloak contestable value judgments in the garb of "science": thus the insatiable demand for mathematical models that reframe subtle and subjective conclusions (such as the worth of a worker, service, article, or product) as the inevitable dictate of salient, measurable data.[26] Big data driven decisions may lead to unprecedented profits. But once we use computation not merely to exercise power over things, but also over people, we need to develop a much more robust ethical framework than "the Blob" is now willing to entertain.

The Secrecy of Business and the Business of Secrecy

Today's finance and Internet companies feverishly sort, rank, and rate. They say they keep techniques strictly secret in order to preserve valuable intellectual property—but their darker motives are also obvious. For example, litigation has revealed that some drug companies have cherry-picked the most positive studies for publication, hiding those with serious health or safety implications.[27] Journalists are prying open Wall Street's pre-financial crisis black boxes to this day.[28] The Sunlight Foundation, Center for Effective Government, AllTrials.net, and Transparency International press for openness.

Politicians are responding, and try to improve disclosure here and there. But they must be cautious. When a gadfly proves too inconve-

nient, companies can band together in a super PAC, funding attacks on the would-be reformer without having to reveal what they are doing until well after the election.[29]

Asked about Google's privacy practices, former CEO Eric Schmidt once said that "Google policy is to get right up to the creepy line and not cross it." It is probably more accurate to say that he and other Silicon Valley leaders don't want to be *caught* crossing the creepy line.[30] As long as secrecy can be used to undermine market competition and law enforcement, they will be emboldened to experiment with ever creepier, more intrusive, and even exploitative practices.

Looking Back

The quest for a more transparent society—more easily understood, and more open about its priorities—has animated leading reformers in the United States. Louis Brandeis's comment that "sunlight is said to be the best of disinfectants," so often cited today, is a century old, dating back to business scandals of the Gilded Age eerily similar to today's casino capitalism.[31] Muckraking journalists and trustbusters of the Progressive Era shamed robber barons by exposing their misdeeds.[32] They targeted politicians, too: the Publicity Act of 1910 mandated disclosure of campaign donations.[33]

Many states of the time took up similar reforms. Voters wanted politics and business subject to public scrutiny. After shady commercial practices surged again in the 1920s, the New Deal echoed and amplified Progressivism. Congress, disgusted by the hucksters who paved the way for the great crash of 1929, imposed sweeping new disclosure obligations in the Securities Act of 1933 and the Securities Exchange Act of 1934. New legislation created the Federal Communications Commission and gave it plenary power to investigate abuses in the telegraph and radio industries.[34] New Deal agencies revealed the inner workings of critical industries.[35]

Government balanced these new powers by opening itself up in important ways. For example, the Administrative Procedure Act (APA) of 1947 forced agencies to give the public notice and a chance to comment before they imposed important rules. Reformers built on the APA with the 1966 Freedom of Information Act, which opened up many government records.[36]

In the 1960s, a broad coalition of interests fought both government and corporate secrecy in the name of citizen empowerment and consumer protection.[37] Perhaps their most enduring legacy was the establishment of procedures of openness. For example, the National Environmental Policy Act required major federal projects to include Environmental Impact Statements that would reveal likely effects on air, water, flora, and fauna. Agencies ranging from the Food and Drug Administration to the Consumer Product Safety Commission now make daily activities less dangerous by revealing the risks of things we purchase.[38]

But there was always pushback. By the late 1960s, businesses were successfully challenging scrutiny from what they branded the "nanny state." When the Environmental Protection Agency wanted to release data on the composition of some pesticides, for example, Monsanto fought back. It won a Supreme Court ruling that prevented the disclosure on the grounds that the formulations were a "trade secret" (a form of intellectual property we'll explore in more detail later). Such rulings chilled many disclosure initiatives, including investigations of Philip Morris's cigarettes and frackers' chemicals.[39]

Confidence in government waned during the stagflation of the 1970s, and business lobbyists seized the opportunity to argue that journalists could do a better job at exposing and punishing corporate wrongdoing than bureaucrats. With zealous investigators ferreting out bad behavior, why bother to require reports? Establishment figures pooh-poohed complaints that banks were becoming too big, complex, and rapacious. "Sophisticated investors" could understand the risks, they insisted, and banks themselves would avoid duplicity to preserve their reputations.[40]

Companies tried to maintain an advantage over their competitors by classifying innovative work as "proprietary" or "confidential." As computerized exchanges made it possible to gain or lose fortunes within seconds, information advantage became critical throughout the economy. Some economists began to question the wisdom of regulating, or even monitoring, the fast-moving corporate world. Some failed to disclose that they were being paid for "consulting" by the same secretive corporations their writings supported. Business

schools taught MBAs the basics of game theory, which stressed the importance of gaining an information advantage over rivals.[41]

Over the last decade, fortunes made via stealth techniques made secrecy even sexier. Google rose to the top of the tech pack while zealously guarding its "secret sauce"—the complex algorithms it used to rank sites. Investment banks and hedge funds made billions of dollars by courting sellers who didn't understand the value of what they were holding and buyers who didn't understand the problems with what they were purchasing.[42]

While neoliberals were vitiating the regulatory state's ability to expose (or even understand) rapidly changing business practices, neoconservatives began to advance a wall of secrecy for the deep state.[43] In the Nixon administration, Dick Cheney and Donald Rumsfeld were already chafing at the idea that Congress could force the executive branch to explain its foreign engagements and strategies. When they renewed their executive service in the George W. Bush administration, they expanded the executive branch's freedom to maneuver (and its power to avoid oversight).[44] After 9/11, they pressed even harder for government secrecy, claiming that the only way to win the "war on terror" was for the state to act as clandestinely as its shadowy enemies.[45]

The Obama administration embraced the expansion of executive secrecy, with far-reaching (and occasionally surreal) results. By 2010, leading intelligence agency experts could not even estimate the overall costs of the U.S. antiterrorism effort; nor could they map the extent of the surveillance apparatus they had built.[46] And their fumbling responses to questions were positively enlightening in comparison with the silence of defense officials funded by the "black budget," whose appropriations only a sliver of Congress and responsible officials are privy to understand.[47] Big government now stands together with security contractors to manage strategic surprise.

Thus the openness mantra of Progressive Era reformers has been neatly reversed in favor of a Faustian (and credulous) bargain: just keep us safe and we won't ask about the details. "Nanny state" takes on a very different connotation in this context.

Things weren't supposed to turn out this way. Little more than a decade ago, the Internet was promising a new era of transparency,

in which open access to information would result in extraordinary liberty. Law professor Glenn Reynolds predicted that "an army of Davids" would overthrow smug, self-satisfied elites. Space physicist David Brin believed that new technology would finally answer the old Roman challenge, "Who will guard the guardians?" But the powerful actors of business, finance, and search did not meekly submit to the fishbowl vision of mutual surveillance that Brin prophesied in *The Transparent Society*. Instead, they deployed strategies of obfuscation and secrecy to consolidate power and wealth.[48] Their opaque technologies are spreading, unmonitored and unregulated.

The Shape of the Book

In this book, I will explore the business practices of leading Internet and finance companies, focusing on their use of proprietary reputation, search, and finance technologies in our often chaotic information environment. In some cases, they enable great gains in efficiency. In others, however, they undermine both economic growth and individual rights.

The success of individuals, businesses, and their products depends heavily on the synthesis of data and perceptions into *reputation*. In ever more settings, reputation is determined by secret algorithms processing inaccessible data. Few of us appreciate the extent of ambient surveillance, and fewer still have access either to its results—the all-important profiles that control so many aspects of our lives—or to the "facts" on which they are based. Chapter 2 illustrates how broadly the new technologies of reputation have infiltrated society.[49]

The more we rely on search engines and social networks to find what we want and need, the more influence they wield. The power to include, exclude, and rank is the power to ensure that certain public impressions become permanent, while others remain fleeting.[50] How does Amazon decide which books to prioritize in searches? How does it ferret out fake or purchased reviews? Why do Facebook and Twitter highlight some political stories or sources at the expense of others?[51] Although internet giants say their algorithms are scientific and neutral tools, it is very difficult to verify those claims.[52] And while they have become critical economic infrastructure, trade secrecy law permits managers to hide their methodolo-

gies, and business practices, deflecting scrutiny.[53] Chapter 3 examines some personal implications of opaque search technology, along with larger issues that it raises in business and law.

Like the reputation and search sectors, the finance industry has characterized more and more decisions as computable, programmable procedures. Big data enables complex pattern recognition techniques to analyze massive data sets. Algorithmic methods of reducing judgment to a series of steps were supposed to rationalize finance, replacing self-serving or biased intermediaries with sound decision frameworks. And they did reduce some inefficiencies. But they also ended up firmly building in some dubious old patterns of credit castes and corporate unaccountability.[54] The black boxes of finance replaced familiar old problems with a triple whammy of technical complexity, real secrecy, and trade secret laws. They contributed to the financial crisis of 2008, according to the *Financial Times*'s John Gapper, because "the opacity and complexity . . . let deception, overpricing and ultimately fraud flourish."[55] Perhaps worse, by naturalizing these (avoidable) features of our social landscape, unregulated financial secrecy is starting to give them a patina of inevitability. Chapter 4 examines the role of opaque models and practices in financial markets, along with the challenges they present to citizens, to society, and to the law.

In his book *Turing's Cathedral*, George Dyson quipped that "Facebook defines who we are, Amazon defines what we want, and Google defines what we think."[56] We can extend that epigram to include *finance*, which defines what we have (materially, at least), and *reputation*, which increasingly defines our opportunities. Leaders in each sector aspire to make these decisions without regulation, appeal, or explanation. If they succeed, our fundamental freedoms and opportunities will be outsourced to systems with few discernible values beyond the enrichment of top managers and shareholders.

This book charts two paths of resistance. Chapter 5 recommends several legal strategies for checking the worst abuses by black box firms. Chapter 6 makes the case for a new politics and economics of reputation, search, and finance, based on the ideal of an intelligible society. It would be foolish to hope for immediate traction in today's gridlocked political environment. But agencies would need to make "all the right moves" within existing legal frameworks to cabin black

box practices. Moreover, those concerned about the power of Silicon Valley and Wall Street need to do more than complain about the limited availability of crucial information. We can imagine a future in which the power of algorithmic authority is limited to environments where it can promote fairness, freedom, and rationality.

We do not have to live in a world where hidden scores determine people's fates, or human manipulations of the stock market remain as inscrutable as the "invisible hand." We should not have to worry that the fates of individuals, businesses, and even our financial systems are at the mercy of hidden databases, dubious scores, and shadowy bets. The same technological and legal revolutions that have so far eviscerated personal privacy can be used to protect it and to advance, rather than curtail, our freedoms and our understanding of the social world. Directed at the right targets, data mining and pervasive surveillance might even prevent the kinds of financial crises and massive misallocations of resources that have devastated the U.S. economy over the past decade.

We need to promote public values in Internet and finance companies, drawing on best practices in other, more regulated sectors. In health care, for example, regulators are deploying technologically savvy contractors to detect and deter fraud, abuse, and unnecessary treatments.[57] Similar techniques can and should be applied to keep banks, search engines, and social networks honest.

More transparency would help outside analysts check "irrational exuberance" in markets and uncover corporate misconduct that is now too easily hidden. It might expose unfair competitive or discriminatory practices. But as I propose regulatory measures, I will repeatedly make the point that transparency is not enough, particularly in the finance sector. When companies parry with complexity too great to monitor or understand, disclosure becomes an empty gesture. We need to put an end to the recursive games of "disclosure" and "tricks to defeat disclosure" that have plagued regulators. Transactions that are too complex to explain to outsiders may well be too complex to be allowed to exist.[58]

The Self-Preventing Prophecy

We need to face the darker possibilities betokened by current trends. There is a venerable fiction genre known as the "self-preventing

prophecy."[59] An author imagines a dystopia, plausibly extrapolating to the future some of the worst trends of the present. If enough readers are shaken from their complacency, they start to make the changes that can prevent the prophecy.[60] The author then avoids the fate of Cassandra, the prophetess of Greek myth whose warnings were fated to be disregarded. George Orwell's *1984* and Aldous Huxley's *Brave New World* could both be understood in this way, helping to mobilize resistance to the totalitarian futures they described.[61]

Films have also aimed for self-preventing prophecy. In Terry Gilliam's *Brazil*, things start to go downhill for protagonist Sam Lowry after a fly accidentally jams a printer at an antiterror agency. As he tries to fix the error, a sclerotic bureaucracy closes in around him, wrongly associating him with violent extremists. Gilliam depicted a state run amok, unaccountable and opaque. Its workings are as mindless and catatonic as the citizens whom it tortures into submission.[62]

We like to believe that we have escaped Gilliam's 1985 dystopia, just as the plausibility of *1984* was eroded by the Eastern Bloc revolutions of 1989. Most major decisions about our lives are made in the private sector, not by a state bureaucracy. State-of-the-art computers are a far cry from the dusty files of the Stasi or the Rube Goldberg contraptions of Gilliam's imagining.[63] The vibrant leaders of Wall Street and Silicon Valley are far more polished than the bumbling and brutal beadles of *Brazil*. Cornucopians urge citizens to simply get out of their way, and to rest assured that technology will solve problems ranging from traffic jams to freakish weather.

But complacency is unwarranted. Many of these companies make decisions affecting millions of people every day, and small mistakes can cascade into life-changing reclassifications. We cannot access critical features of their decision-making processes. The corporate strategists and governmental authorities of the future will deploy their massive resources to keep their one-way mirrors in place; the advantages conferred upon them by Big Data technologies are too great to give up without a fight. But black boxes are a signal that information imbalances have gone too far. We have come to rely on the titans of reputation, search, and finance to help us make sense of the world; it is time for policymakers to help us make sense of the sensemakers.

In their workplaces and in their homes, Americans are increasingly influenced—some might say bullied—by managers who keep their methods under wraps. Corporations depend on automated judgments that may be wrong, biased, or destructive. The black boxes of reputation, search, and finance endanger all of us. Faulty data, invalid assumptions, and defective models can't be corrected when they are hidden. This book exposes them, and proposes solutions.

2

DIGITAL REPUTATION IN AN ERA OF RUNAWAY DATA

TELL US EVERYTHING, Big Data croons. Don't be shy. The more you tell us, the more we can help you. It's like the Elf on the Shelf, whom Santa deputizes to do his holiday watching. It sits and reports—naughty or nice? It can move around, the better to see, but only when the kids aren't looking. If they touch the elf, its magic is lost. But for the obedient, Christmas presents await!

While most kids don't believe in the elf past the age of reason, policymakers are still buying into Big Data's myths. Too many consumers do, too. Eric Schmidt says that he wants Google users to be able to ask it, "'What shall I do tomorrow?' and 'What job shall I take?'," and users barely raise an eyebrow about the implications of giving one company such intimate knowledge about their lives. Given optimal personalization and optimal data points, Big Data will plan for us an optimal life. And it costs us nothing!

Except that's the myth. For every discount or shortcut big data may offer, it's probably imposing other, hidden costs or wild goose chases. Your data is a source of huge profit to other people, but often at your expense. In the wrong hands, your data will cost you dearly.[1]

Data-intensive advertising helps generate over $150 billion a year in economic activity.[2] Boosters claim that it gives us an ever more personalized, user-friendly Internet. But advertising companies,

and the people who pay them, aren't in business for their health. They're looking for profit. When we click on an ad promising a discount, there's probably a program behind the scenes calculating how much more it can charge us on the basis of our location,[3] or whether we're using a Mac or PC, or even court records.[4] It's not only the National Security Agency (NSA) that covets total information awareness; that's the goal of marketers, too. They want that endless array of data points to develop exhaustive profiles. Of us.

Pattern recognition is the name of the game—connecting the dots of past behavior to predict the future. Are you a fierce comparison shopper, or the relaxed kind who's OK spending a few extra dollars for a plane ticket or a movie if it saves some trouble? Firms want to know, and they can find out quite easily. Every business wants a data advantage that will let it target its ideal customers.

Sometimes the results are prosaic and predictable: your favorite retailer may pop up as an ad on every other website you visit. But that's the tip of an iceberg of marketing. What lies beneath are myriad unsavory strategies. One data broker sold the names of 500,000 gamblers over 55 years old for 8.5 cents apiece to criminals, who then bilked money from vulnerable seekers of "luck." Others offered lists of patients with cancer or Alzheimer's disease.[5] Firms can "refine" such lists, seeking out the gullible and the desperate. They aren't just the bottom feeders on the margins of the economy, either. Google is a "go-to" firm for digital marketing because it knows us so well—naughty or nice, wise or foolish, good credit or bad.[6] And a surprising proportion of digital marketing is about finding marks for dubious loans, pharmaceutical products, and fly-by-night for-profit educators.[7]

Businesses are looking for the cheapest, most cost-effective workers, too. They scrutinize our work records the way they scour our online data trails. This data analysis is usually framed as a way of rewarding high performers and shaming shirkers. But it's not so simple. Most of us don't know that we're being profiled, or, if we do, how the profiling works. We can't anticipate, for instance, when an apparently innocuous action—like joining the wrong group on Facebook—will trigger a red flag on some background checker that renders us effectively unemployable.

We also don't know much about *how* data from one sphere feeds into another: as the Federal Trade Commission has concluded, there is "a fundamental lack of transparency about data broker industry practices."[8] We do know that it does. Law enforcement, for example, can enlist the help of our bosses—and of Big Data—to keep an eye on us. The Fourth Amendment puts some (minimal) constraints on government searches of our records, but does not apply to employers. One woman, using a computer that belonged to her employer, searched for "pressure cookers" in the same time frame that her husband searched for "backpacks." Though she'd left the company, her employer was still reporting "suspicious activities" on its machines to local police. Six agents, two of whom identified themselves as members of the government's regional Joint Terrorism Task Force, came to visit her.[9]

As complaints, investigations, and leaks give us occasional peeks into the black boxes of reputation analysis, a picture of decontextualized, out-of-control data mining emerges. Data brokers can use private and public records—of marriage, divorce, home purchases, voting, or thousands of others—to draw inferences about any of us. Laws prevent government itself from collecting certain types of information, but data brokers are not so constrained. And little stops the government from *buying* that information once it's been collected. Thus commercial and government "dataveillance" results in synergistic swapping of intimate details about individual lives.[10]

America's patchwork of weak privacy laws are no match for the threats posed by this runaway data, which is used secretly to rank, rate, and evaluate persons, often to their detriment and often unfairly. Without a society-wide commitment to fair data practices, digital discrimination will only intensify.

On (and beyond) Data

Even with that commitment, we can't forget that access to data is just the first and smallest step toward fairness in a world of pervasive digital scoring, where many of our daily activities are processed as "signals" for rewards or penalties, benefits or burdens. Critical decisions are made not on the basis of the data per se, but on the basis of data analyzed *algorithmically:* that is, in calculations coded in

computer software. Failing clear understanding of the algorithms involved—and the right to challenge unfair ones—disclosure of underlying data will do little to secure reputational justice. Here a familiar concept from personal finance—the credit score—can help illuminate the promise and pitfalls of a "scored" world.

From Credit History to Score: The Original Black Box. Credit bureaus pioneered black box techniques, making critical judgments about people, but hiding their methods of data collection and analysis. In the 1960s, innuendo percolated into reports filed by untrained "investigators." They included attributes like messiness, poorly kept yards, and "effeminate gestures."[11] The surveillance could be creepy and unfair—virtually everyone has some habit that could be seized on as evidence of unreliability or worse. Combine the lax standards for reporting with a toxic mix of prejudices common at the time, and the flaws of this system are obvious.

News reports on credit bureaus were alarming enough that in 1970, Congress passed the Fair Credit Reporting Act (FCRA), which required that the bureaus make their dossiers both accurate and relevant.[12] Credit bureaus' files were opened to scrutiny, and consumers were given the right to inspect their records and demand corrections.[13] This dose of sunlight was a decent disinfectant as far as relevance was concerned; questionable characterizations of sexual orientation and housekeeping faded out of bureau reports as people gained access to their profiles.

However, the right to dispute credit bureau records did not, and does not, guarantee accuracy. In a report for *60 Minutes*, journalist Steve Kroft described a conversation with a "dispute agent" at one of the large credit bureaus. His informant bluntly admitted the prevailing attitude that "the creditor was always right."[14] Agents said their bureau asked them to review ninety cases a day, which averages out to less than six minutes per case. And even when they had the opportunity to get to the bottom of things, they had little power to resolve the matter in favor of the consumer. Little wonder, then, that Kroft's report exposed an avalanche of complaints against the industry.

Though bureaus complained *60 Minutes* was unfair, their track record is not exactly sterling. Reports show that credit bureaus have

strived mightily to deflect minimal demands for accountability.[15] For example, after federal law required them to release to consumers an annual free copy of their credit histories via the site AnnualCreditReport.com, bureaus set up "FreeCreditReport.com" to lull the unsuspecting into buying expensive credit monitoring services.[16] Decoy websites proliferated.[17] To minimize the visibility of the real site, www.annualcreditreport.com, the bureaus "blocked web links from reputable consumer sites such as Privacy Rights Clearinghouse, and Consumers Union, and from mainstream news web sites."[18] Enforcers at the Federal Trade Commission had to intervene in 2005, but the penalties imposed (a tiny fraction of the revenues generated by the deceptive practice) could not possibly have a serious deterrent effect.[19]

The story gets even more depressing when we consider that, by the time the United States got relatively serious about making credit *reporting* transparent, credit *scores* were more important—and still largely black-boxed. Banks and credit card issuers use the scores to predict the likelihood of borrowers to default on their debts.[20] A bad score can mean significantly higher interest rates. But critics have called the scores opaque, arbitrary, and discriminatory, and there is little evidence scorers are doing much to respond to these concerns.[21]

That's an uncomfortable reality in a world where credit scores have escaped from their native financial context and established themselves as arbiters of general reliability in other areas, like car insurance.[22] An unemployed person with a poor credit history, not necessarily through his own fault, is likely to find it harder to find the work needed to earn the money to pay off his debts.[23] If he fails to, his credit history will further deteriorate, his interest rates will go up, and a vicious cycle ensues. The credit score is too powerful a determiner of success and failure to be allowed to do its work in secrecy.[24]

In 2010, in the aftermath of the subprime mortgage meltdown, many homeowners wanted to know who actually owned their mortgages,[25] and a website called "Where's the Note" offered information on how to force servicers to prove that they had legal rights to mortgage payments.[26] Given the unprecedented level of foreclosure

fraud, sloppy paperwork, and "robo-signed" affidavits revealed during the crisis, one might think that a sensible credit scoring system would reward those who took the trouble to verify the status of their financing.[27] But participants in online forums worry that the opposite is the case.[28] A homeowner who followed the instructions on "Where's the Note" reported that he took a 40-point hit on his credit score after his inquiry.[29] In the Heisenberg-meets-Kafka world of credit scoring, merely trying to figure out possible effects on one's score can reduce it.

Scoring is just comprehensible enough to look like a fair game. But it's opaque enough that only insiders really know the rules. FICO and the credit bureaus promote their systems as models of fairness, but justify them with generalities.[30] They peddle bromides: pay your debts on time; don't push against the upper bounds of your credit limit, but don't eschew credit entirely; build up a record so your credit history can be scored.[31] There are dozens of self-help books and pamphlets on the topic.[32] Internet groups like "FICO Forums" discuss the practices of the credit card companies and try to reverse engineer their scoring decisions.[33] But even the most faithful student of these mysteries is never really going to be able to predict the exact consequences of his actions.

Three credit bureaus, Experian, TransUnion, and Equifax, routinely score millions of individuals.[34] But not always the same way. In one study of 500,000 files, "29% of consumers [had] credit scores that differ by at least fifty points between credit bureaus."[35] Fifty points can mean tens of thousands of dollars in extra payments over the life of a mortgage; unless the aims of the different bureaus diverge in undisclosed ways, so much variation suggests that the assessment process is more than a little arbitrary. The experience of the "Where's the Note" man is an egregious example of its unpredictability, but there are easier ways for responsible people to get into trouble when the rules aren't stated. A consumer might reduce his limit on a credit card with the intent of limiting his exposure to fraud or even his own spending. If he doesn't know that the bureaus tend to favor those who use a smaller proportion of their existing credit,[36] he may be surprised to see the resulting increase of the card's "debt-to-limit ratio" ding his score instead of rewarding his prudence.[37]

So while the public face of credit evaluation is a three-digit number, a marvel of concrete and compact clarity, beneath that appealing surface is a process that cannot be fully understood, challenged, or audited either by the individuals scored or by the regulators charged with protecting them. One expert observes that the inevitable subjectivity of these black box assessments is rendered "hidden and incontestable by the apparent simplicity of [that] single figure."[38] The number may *feel* as objective and real as the score on a math test. But a critical mass of complaints over the past twenty years has eroded credit assessors' claims to objectivity and reliability.[39]

The Scored Society. Many grievances arise out of the growing influence of secret credit scoring algorithms as an all-purpose reputational metric.[40] But at least the data and rough outlines of credit scoring procedures are regulated and disclosed. Another world of consumer profiling—ranging from ad networks to consumer scores—is barely touched by law. They revive some of the worst aspects of unregulated credit reporting, but well out of the public eye.

The credit bureaus aren't intuiting our sexual orientations anymore, or rating us by our housekeeping. Still, there's money to be made from knowing if someone is gay, or how well they keep their property up, or if they have property at all. Marketers crave that information, and the vacuum left by the bureaus has been filled by a behind-the-scenes cohort of unregulated data gatherers, brokers, sensor networks, and analysts who collect and scrutinize every bit of spoor, digital and otherwise, that we leave behind.

As far back as 2002, a digital video recorder (DVR) took it upon itself to save a number of gay-themed shows for its owner after he recorded a film with a bisexual character in it.[41] The owner persuaded it (that is, he sent the right signals to the algorithm encoded in its software) to revise its "opinion" by recording something from the Playboy Channel. Big Data partisans would doubtless argue that with *more* data the machine could have made more accurate predictions before. But the telling point for the rest of us is that the machine had that data at all—and power to make use of it.

That power has spread to many online contexts. One MIT study concluded that gay men "can be identified by their Facebook

friends,"[42] and bots can plunder social networks for their wealth of clues to sexual orientation. One closeted user who left a positive comment on a story on gay marriage found himself targeted by a rainbow-underwear-emblazoned ad for a "Coming Out Coach."[43]

The United States is at last entering an era where being gay is less of a stigma than it has been; some might even laugh off the rainbow underwear as a welcome sign of inclusion. But imagine how the information might be used in Russia. Moreover, plenty of characterizations are indisputably damaging or sensitive in any context. OfficeMax once accidentally sent a mailing addressed to "Mike Seay, Daughter Killed in Car Crash." Seay's daughter had indeed died in a car accident less than a year before.[44] How or why this piece of creepiness could have been relevant to OfficeMax's marketing strategy is anybody's guess. The company is not telling. It's not revealing where it got its information from, either. Data brokers can oblige customers contractually not to reveal them as sources.[45] The shadowy masters of industrial data mining eviscerate personal privacy from behind a veil of corporate secrecy. We'll see this dynamic repeatedly: corporate secrecy expands as the privacy of human beings contracts.

Runaway data isn't only creepy. It can have real costs. Scoring is spreading rapidly from finance to more intimate fields. Health scores already exist, and a "body score" may someday be even more important than your credit score.[46] Mobile medical apps and social networks offer powerful opportunities to find support, form communities, and address health issues. But they also offer unprecedented surveillance of health data, largely ungoverned by traditional health privacy laws (which focus on doctors, hospitals, and insurers).[47] Furthermore, they open the door to frightening and manipulative uses of that data by ranking intermediaries—data scorers and brokers—and the businesses, employers, and government agencies they inform.[48]

Even regulated health data can pop up in unexpected ways. Consider the plight of Walter and Paula Shelton, a Louisiana couple who sought health insurance.[49] 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? And even if they had known, what should they, or their doctor, have done? Indeed, the model for blackballing them might well still have been a gleam in an entrepreneur's eye when Mrs. Shelton obtained her medications. 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.[50]

Chad Terhune, the journalist who in 2008 first reported on the Sheltons, detailed the many ways that prescription data was being used in the individual insurance market. Companies were gathering millions of records from pharmacies.[51] They then sold them on to insurers eager to gain a competitive advantage by avoiding people likely to incur high medical fees. Since 1 percent of patients account for over one-fifth of health care costs, and 5 percent account for nearly half of costs, insurers who can "cherry-pick" the healthy and "lemon-drop" the sick will see far more profit than those who take all comers.[52] Prescription data gave insurers the information they needed to tailor policies to exclude preexisting conditions and to impose higher charges for some members.

Ironically, this kind of data was originally gathered to help patients in emergency care settings—to assure access to a record of their medications. But when that plan failed, the records were quietly repurposed as a means of discriminating against the sick. If there's one thing Wall Street loves, it's a quick pivot to a winning business strategy.

From Medical Record to Medical Reputation. Given the passage of the Affordable Care Act (ACA), those with a long history of prescriptions do not have quite as much to worry about in the health insurance market: insurers cannot discriminate on the basis of pre-existing conditions now.[53] But other opportunities may be foreclosed. Moreover, the ACA also includes provisions promoting insurance discounts in exchange for participation in "wellness programs." Verifying that participation (in activities ranging from meditation to

running) can only expand the market for bodily surveillance and quantified selves.

Medical reputations are being created in processes we can barely understand, let alone control.[54] And in an era of Big Data, companies don't even need to consult physicians' records to impute to us medical conditions and act accordingly. Do a few searches about a disease online, fill out an (apparently unrelated) form, and you may well end up associated with that disease in commercial databases.

An insightful reporter documented that process with a (healthy) friend who received a mystifying invite to a meeting of multiple sclerosis patients. Apparently the (non)patient had filled out a registration form, and the data was harvested and sold to a marketing company.[55] She still doesn't know exactly what they found on it, or whether the form warned her about this type of use (imagine trying to recall all the terms of service you've clicked through without reading). But the marketer sold it to MS LifeLines®, a support network owned by two drug companies. The first time she had any inkling of any of this was when she received the promotional materials for the MS event. How many of the rest of us are mysteriously "weblined" into categories we know nothing about?[56]

Even the partial exposure of such data transfers is unusual. In most cases, they stay well hidden. But reporters are beginning to open up the black box of consumer profiling, as Charles Duhigg did in his 2012 report on Target, the second-largest U.S. discount retailer and a company that prides itself on knowing when its customers are pregnant.[57] For a retailer of that size, the pattern recognition was easy. First, Target's statisticians compiled a database of "the known pregnant"—people who had signed up for baby registries. Then they compared the purchases of consumers in that data set to the purchases made by Target shoppers as a whole. (Every Target shopper has a "Guest ID" number, tied to credit card, e-mail address, and other such identifiers.) By analyzing where the pregnant shoppers diverged the most from the general data set, they identified "signals" of pregnancy-related purchases.

In the first twenty weeks, "supplements like calcium, magnesium and zinc" were a tip-off. Later in the pregnancy, "scent-free soap and extra-big bags of cotton balls" were common purchases. By the

end of the analysis, the statisticians had incorporated a list of twenty-five products into a "pregnancy prediction score" and due-date estimator; if a twenty-three-year old woman in Atlanta bought "cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug" in March, Target estimated an 87 percent chance that she was pregnant and due to give birth in late August. Not surprisingly, some customers found it creepy to start receiving pregnancy-related ads. Target responded, not by explaining to customers how it came to its conclusions, but by mixing more non-pregnancy-related ads into the circulars targeting expectant mothers.

We don't know what other health-related categories Target slices and dices its customers into. It stopped talking to Duhigg, and it probably considers its other methods (and categories) valuable trade secrets. But about two years later, Target suffered a data breach—one of the largest in retail history. It affected an estimated 110 million people. Hackers stole "mailing and email addresses, phone numbers or names, [and] the kind of data routinely collected from customers during interactions like shopping online."[58] Lots of customers found *that* creepy—and scary, too, given how much data retailers routinely collect. Imagine what sub rosa data brokers could do with comprehensive customer profiles.[59]

The growing danger of breaches challenges any simple attempts to justify data collection in the service of "consumer targeting." Even huge and sophisticated companies can be hacked, and cybercriminals' data trafficking is, unsurprisingly, an obscure topic.[60] In at least one case, an established U.S. data broker accidentally sold "Social Security and driver's license numbers—as well as bank account and credit card data on millions of Americans" to ID thieves.[61] Until data companies are willing to document and report the precise origins and destinations of all the data they hold, we will never be able to estimate the magnitude of data misuse.

Big data enables big dangers. Are the present benefits worth the long-term costs? Perhaps. Some pregnant moms-to-be may be thrilled to get coupons tailored precisely to them. But not the teen who hadn't yet told her father that she was pregnant.[62] And probably not the people who type words like "sick," "stressed," or "crying"

into a search engine or an online support forum and find themselves in the crosshairs of clever marketers looking to capitalize on depression and insecurity.[63] Marketers plot to tout beauty products at moments of the day that women feel least attractive.[64] There's little to stop them from compiling digital dossiers of the vulnerabilities of each of us.[65] In the hall of mirrors of online marketing, discrimination can easily masquerade as innovation.

These methods may seem crude or reductive, but they are beloved by digital marketers. They are fast and cheap and there is little to lose. Once the data is in hand, the permutations are endless, and somebody is going to want them. If you're a childless man who shops for clothing online, spends a lot on cable TV, and drives a minivan, we know that data brokers are going to assume you're fatter than the average person.[66] And we now know that recruiters for obesity drug trials will happily pay for that analysis, thanks to innovative reporting.[67] But in most cases, we don't know what the brokers are saying about us. And since a data breach could spill it open to the world at large, it would be nice if we did.

Runaway Profiles

Where does all this data come from? Everywhere. Have you ever searched for "flu symptoms" or "condoms"? That clickstream may be around somewhere, potentially tied to your name (if you were signed in) or the IP address of your computer or perhaps some unique identifier of its hardware.[68] It's a cinch for companies to compile lists of chronic dieters, or people with hay fever. "Based on your credit-card history, and whether you drive an American automobile and several other lifestyle factors, we can get a very, very close bead on whether or not you have the disease state we're looking at," said a vice president at a company in the health sector.[69]

Other companies sell the mailing addresses and medication lists of depressed people and cancer patients. A firm reportedly combines credit scores and a person's specific ailments into one report.[70] The Federal Trade Commission is trying to nail down a solid picture of these practices, but exchange of health data is an elusive target when millions of digital files can be encrypted and transmitted at the touch of a button.[71] We may eventually find records of data *sales*,

but what if it is traded in handshake deals among brokers? A stray flash drive could hold millions of records. It's hard enough for the agency to monitor America's brick-and-mortar businesses; the proliferation of data firms has completely overtaxed it.[72] Consider a small sample of the sources that can collect information about a person, in the table below.

Table 2.1 separates information-collecting sources into specific sectors, denoting only their *primary* activities, not all the inferences they make by way of the data they compile. For example, we already know that at least one credit card company pays attention to certain mental health events, like going to marriage counseling.[73] When statistics imply that couples in counseling are more likely to divorce than couples who aren't, counseling becomes a "signal" that marital discord may be about to spill over into financial distress.[74] This is effectively a "marriage counseling penalty" and poses a dilemma for policy makers. Left unrevealed, it leaves cardholders in the dark about an important aspect of creditworthiness. Once disclosed, it could discourage a couple from seeking the counseling they need to save their relationship.

Table 2.1. A Glimpse of the Data Tracking Landscape

	Health	Finance	Retail
First Party (self-tracking)	Weight loss or exercise app on phone	Home finance software	Self-monitoring of purchases
Second Party (direct interaction)	Amazon logs purchase of diet books	Purchase of Turbotax® online	Target or Amazon logs purchases in company database
Third Party (intermediary logging data)	ISP or search engine logs queries about diabetes, cancer, other diseases	Credit card company analyzes transactions between first party (you) and sellers (second party)	Cookies from ad networks or social networks may be logging records of items reviewed
Fourth Party (broker buying data from any of the above)	*Data brokers increasingly try to integrate all of the aforementioned sources into profiles. They help create a competitive landscape where leading second- and third-party firms also feel the need to integrate data.*		

There doesn't have to be any established causal relationship between counseling and late payments; correlation is enough to drive action. That can be creepy in the case of objectively verifiable conditions, like pregnancy. And it can be devastating for those categorized as "lazy," "unreliable," "struggling," or worse. Runaway data can lead to *cascading disadvantages* as digital alchemy creates new analog realities. Once one piece of software has inferred that a person is a bad credit risk, a shirking worker, or a marginal consumer, that attribute may appear with decision-making clout in other systems all over the economy. There is little in current law to prevent companies from selling their profiles of you.[75]

Bad inferences are a larger problem than bad data because companies can represent them as "opinion" rather than fact. A lie can be litigated, but an opinion is much harder to prove false; therefore, under the First Amendment to the U.S. Constitution, it is much harder to dispute.[76] For example, a firm may identify a data subject not as an "allergy sufferer," but as a person with an "online search propensity" for a certain "ailment or prescription."[77] Similar classifications exist for "diabetic-concerned households." It may be easy for me to prove that I don't suffer from diabetes, but how do I prove that I'm not "diabetic-concerned"? And if data buyers are going to lump me in with diabetics anyway, what good does it do me even to bother challenging the record?

Profiling may begin with the original collectors of the information, but it can be elaborated by numerous data brokers, including credit bureaus, analytics firms, catalog co-ops, direct marketers, list brokers, affiliates, and others.[78] Brokers combine, swap, and recombine the data they acquire into new profiles, which they can then sell back to the original collectors or to other firms. It's a complicated picture, and even experts have a tough time keeping on top of exactly how data flows in the new economy.

A Thousand Eyes. Most of us have enough trouble keeping tabs on our credit history at the three major credit bureaus. But the Internet has supercharged the world of data exchange and profiling, and Experian, TransUnion, and Equifax are no longer the sole, or even the main, keepers of our online reputations. What will hap-

pen when we've got dozens, or hundreds, of entities to keep our eyes on?

We're finding out. They're already here, maintaining databases that, though mostly unknown to us, record nearly every aspect of our lives. They score us to decide whether we're targets or "waste," as media scholar Joseph Turow puts it.[79] They keep track of our occupations and preoccupations, our salaries, our home value, even our past purchases of luxury goods.[80] (Who knew that one splurge on a pair of really nice headphones could lead to higher prices on sneakers in a later online search?) There are now hundreds of credit scores for sale, and thousands of "consumer scores," on subjects ranging from frailty to reliability to likelihood to commit fraud. And there are far more sources of data for all these scores than there are scores themselves.[81]

ChexSystems and TeleCheck track bounced checks; Alliant Cooperative Data Solutions documents missed monthly payments for gym memberships; payday lenders report "deadbeats" to Teletrack. Datalogix has lists of dieters. The National Consumer Telecom and Utilities Exchange uses data from several large companies to set recommended deposits for cable and utility subscribers but would not reveal to a reporter the names of those data-gathering companies. Reporting agencies monitor our utility bills, our rent payments, and our medical debts. Any one of them could change our lives on the basis of a falsehood or a mistake that we don't even know about.

For example, one data broker (ChoicePoint) incorrectly reported a criminal charge of "intent to sell and manufacture methamphetamines" in Arkansas resident Catherine Taylor's file. The free-floating lie ensured rapid rejection of her job applications. She couldn't obtain credit to buy a dishwasher. Once notified of the error, ChoicePoint corrected it, but the other companies to whom ChoicePoint had sold Taylor's file did not necessarily follow suit. Some corrected their reports in a timely manner, but Taylor had to repeatedly nag many others, and ended up suing one.[82]

Taylor found the effort to correct all the meth conviction entries overwhelming. "I can't be the watchdog all the time," she told a *Washington Post* reporter. It took her four years to find a job even after the error was uncovered, and she was still rejected for an apartment. She

ended up living in her sister's house, and she claims that the stress of the situation exacerbated her heart problems.

For every Catherine Taylor, who was actually aware of the data defaming her, there are surely thousands of us who don't know that there are scarlet letters emblazoned on our digital dossiers. It doesn't even occur to us that there might be anything to investigate. But even when the lies lead not to outright denials, but only to slightly worse credit rates or job opportunities, we suffer from them nonetheless.[83]

Big Data at Work

Big Data dominates big workplaces, too, from the moment we make our first approach to an employer to the day we leave. Companies faced with tens of thousands of job applications don't want to deal with each one individually. It's easier and faster to let software programs crunch a few hundred variables first. There are online evaluation systems that score interviewees with color-coded ratings; red signals a candidate as poor, yellow as middling, and green as likely hires.[84] Some look at an applicant's life online,[85] ranking candidates on the creativity, leadership, and temperament evidenced on social networks and search results.[86] As with credit scoring, the new world of social scoring creates demand for coaching. (Better think twice about using three exclamation marks on a Facebook comment. But be sure to have *some* Facebook activity, lest you look like a hermit.)[87] Tools of assessment range from the obvious and transparent to the subtle and hidden. One company completed investigations for 4,000-plus employers, with almost no oversight from its clients or challenge from its subjects.[88]

Once we're in, firms like Recorded Future, partly funded by arms of Google and the CIA, offer more sophisticated techniques of data analysis to protect bosses from hirer's remorse.[89] "They're Watching You at Work," intoned *The Atlantic* in a compilation of examples of pervasive monitoring. (One casino tracks how often its card dealers and waitstaff smile.) Analysts mine our e-mails for "insights about our productivity, our treatment of co-workers, our willingness to collaborate or lend a hand, our patterns of written language, and what those patterns reveal about our intelligence, social skills, and behavior."[90]

Whatever prerogatives we may have had when we walked in the door, we sign many of them away just filling out the now-standard HR forms.[91] Workers routinely surrender the right to object to, or even know about, surveillance.[92] "Consent is the universal solvent," one employment lawyer told me matter-of-factly. Technology makes it easy for firms to record workers' keystrokes and telephone conversations, and even to translate speech into text and so, predictive analysts claim, distinguish workers from shirkers. Call centers are the ultimate embodiment of the panoptic workspace. There, workers are monitored all the time. Similar software analyzes callers simultaneously, matching them to agents via emotion-parsing algorithms. Sound furious as you talk your way through a phone tree, and you may be routed to someone with anger management training. Or not; some companies work extra hard to soothe, but others just dump problem customers. There's a fine line between the wooed and the waste.

"Data-driven" management promises a hyperefficient workplace. The most watched jobs are also the easiest to automate: a comprehensive documentation of everything a worker has done is the key data enabling a robot to take her place.[93] But good luck finding out exactly how management protocols work. If they were revealed, the bosses claim, employees would game the system. If workers knew that thirty-three-word e-mails littered with emoticons scored highest, they might write that way all the time. Thus a new source of tension arises: workers want and need to learn the rules of success at a new workplace, but management worries that if the rules are known, they'll lose their predictive value.

The Fair, the Foul, and the Creepy. Automated systems claim to rate all individuals the same way, thus averting discrimination. They may ensure some bosses no longer base hiring and firing decisions on hunches, impressions, or prejudices.[94] But software engineers construct the datasets mined by scoring systems; they define the parameters of data-mining analyses; they create the clusters, links, and decision trees applied; they generate the predictive models applied. Human biases and values are embedded into each and every step of development. Computerization may simply drive discrimination upstream.

Moreover, even in spheres where algorithms solve some problems, they are creating others. Wharton Business School professor Peter Cappelli believes firms are relying "too much on software to screen thousands of applications, which dooms promising candidates whose resumes lack the precise words that alert such programs."[95] Bewitched by matching and sorting programs, a company may treat ever more hires as "purple squirrels"—an HR term of art denoting the *exact* perfect fit for a given position. For example, consider a health lawyer qualified to work on matters involving Zone Program Integrity Contractors, but who does not use the specific acronym "ZPIC" on her resume. If automated software is set to search only for resumes that contain "ZPIC," she's probably not going to get an interview. She may never find out that this small omission was the main, or only, reason she never got a callback. Cappelli considers automated resume-sorting software an insurmountable barrier for some qualified persons looking for good jobs.[96]

Then there's the growing use of personality tests by retailers. In an era of persistently high unemployment, even low-wage cashier and stocking jobs are fiercely competitive.[97] Firms use tests to determine who is a good fit for a given job. Writer Barbara Ehrenreich encountered one of those tests when she applied for a job at Walmart, and she was penalized for agreeing "strongly" rather than "totally" with this statement: "All rules must be followed to the letter at all times."[98] Here are some other statements from recent pre-employment tests. There are four possible multiple-choice answers: strongly disagree, disagree, agree, and strongly agree.

- You would like a job that is quiet and predictable.
- Other people's feelings are their own business.
- Realistically, some of your projects will never be finished.
- You feel nervous when there are demands you can't meet.
- It bothers you when something unexpected disrupts your day.
- In school, you were one of the best students.
- In your free time, you go out more than stay home.[99]

How would you respond to questions like those? What on earth do they imply about a would-be clerk, manager, or barista? It's not

readily apparent. Yet despite their indeterminacy, these tests have important consequences for job seekers. Applicants with a "green score" have a decent shot at full interviews; those in the "red" or "yellow" zone are most likely shut out.

One of these black box personality tests was used in 16 percent of major retail hiring in 2009, and at least one manager seemed to share Ehrenreich's view that it selected for soulless sycophants. "A lot of people who score green just figured out how to cheat the system, or are just the 'yes' people," she said. "I don't believe it makes them more capable than anyone else."

Profiling's proponents counter that there's no need to explain *how* the answers in a particular questionnaire correspond to performance, as long as we know *that they do*.[100] They aren't really trying to assess competence or overall job ability. The test is only one part of a multistep hiring process, designed to predict how likely a new hire is to succeed.[101] For example, a company might find that every applicant who answered "strongly agree" to all the questions above turned out to be a model employee, and those who answered "strongly disagree" ended up quitting or being fired within a month or two. The HR department would be sorely tempted to hire future applicants who "strongly agreed," even without knowing *how* such professed attitudes related to the job at hand.

However useful they may be to employers, black box personality tests are unsettling to applicants. Correctness aside, on what grounds do employers get to ask, "How nervous are you when there are demands you can't meet?" Why do nerves matter if an employee can flawlessly complete the given job nevertheless? We want and need reasons for the ways we are treated, even when they are curt or blunt.[102] Is the "reasoning" behind questions like this the kind of decision making that should decide people's fates?

Secret statistical methods for picking and assessing employees seem to promise a competitive edge. Whether these methods deliver or not is unclear, and they feel "creepy" to many workers, who fear having a critical aspect of their lives left to mysterious and unaccountable computer programs.[103] Employers invested in these technologies pooh-pooh the "creepiness" objection as a matter of taste or a regrettable lack of the toughness the work world requires. But the creepy feeling is world disclosive; it is an emotional reaction

that alerts us to the possibility of real harm.[104] Employers and data analysts have become partners in the assembly of ostensible "realities" that have serious life consequences for the individuals they purport to describe. Yet these individuals have no idea how the "realities" are being constructed, what is in them, or what might be done with them. Their alarm is warranted.[105]

The Specter of Racial Bias

Anyone may be labeled in a database as "unreliable," "high medical cost," "declining income," or some other derogatory term. Reputation systems are creating new (and largely invisible) minorities, disfavored due to error or unfairness. Algorithms are not immune from the fundamental problem of discrimination, in which negative and baseless assumptions congeal into prejudice. They are programmed by human beings, whose values are embedded into their software.[106] And they must often use data laced with all-too-human prejudice.

There are some partisans of the "reputation society" who acknowledge that all the data mining can get a little creepy sometimes. But, they promise, it's better than the alternative. They fault hiring and promotion decisions made the old-fashioned way—based on in-person interviews and human review of a resume—as more biased than automated judgments.[107] University of Chicago law professor Lior Strahilevitz thinks that "reputation tracking tools . . . provide detailed information about individuals, thereby reducing the temptation for decision makers to rely on group-based stereotypes."[108] He endorses the use of criminal background histories in hiring. But he does not adequately acknowledge the degree to which such sources can be based on biased data—for example, if police focus their efforts on minority communities, more minorities may end up with criminal records, regardless of whether minorities generally commit more crimes.[109] Researchers are revealing that online sources may be just as problematic. As the White House Report on Big Data has found, "big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace."[110] Already disadvantaged groups may be particularly hard hit.[111]

For example, consider one computer scientist's scrutiny of digital name searches. In 2012, Latanya Sweeney, former director of the Data Privacy Lab at Harvard and now a senior technologist at the Federal Trade Commission, suspected that African Americans were being unfairly targeted by an online service. When Sweeney searched her own name on Google, she saw an ad saying, "Latanya Sweeney: Arrested?" In contrast, a search for "Tanya Smith" produced an ad saying, "Located: Tanya Smith."[112] The discrepancy provoked Sweeney to conduct a study of how names affected the ads served. She suspected that "ads suggesting arrest tend to appear with names associated with blacks, and neutral ads or no [such] ads tend to appear with names associated with whites, regardless of whether the company [purchasing the ad] has an arrest record associated with the name." She concluded that "Google searches for typically African-American names lead to negative ads posted by [the background check site] InstantCheckmate.com, while typically Caucasian names draw neutral ads."[113]

After Sweeney released her findings, several explanations for her results were proposed. Perhaps someone had deliberately programmed "arrest" results to appear with names associated with blacks? That would be intentional discrimination, and Instant Checkmate and Google both vehemently denied it. On the other hand, let us suppose that (for whatever reasons) web searchers tended to click on Instant Checkmate ads more often when names associated with blacks had "arrest" associations, rather than more neutral ones. In that case, the programmer behind the ad-matching engine could say that all it is doing is optimizing for clicks—it is agnostic about people's reasons for clicking.[114] It presents itself as a cultural voting machine, merely registering, rather than creating, perceptions.[115]

Given algorithmic secrecy, it's impossible to know exactly what's going on here. Perhaps a company had racially inflected ad targeting; perhaps Sweeney's results arose from other associations in the data. But without access to the underlying coding and data, it is nearly impossible to adjudicate the dispute.

It would be easier to give tech companies the benefit of the doubt if Silicon Valley's own diversity record weren't so dismal. Google

and other tech companies refused to reveal the demographic makeup for their own workforces for years, calling it a trade secret. When Google finally did reveal the numbers, critics were concerned: only 2 percent of its 46,000 or so U.S. employees were African American (compared with 12 percent of the U.S. workforce).[116] Might the lack of representation of minorities inside the company help explain its dismissive responses?

A similar controversy, involving Google's Gmail, is not encouraging. That service also aggregates information to target ads to users. Researcher Nathan Newman created a number of test Gmail accounts. He then compared the ad results delivered to different-sounding names when he sent e-mails about car shopping to and from the test accounts. He found that "all three white names yielded car buying sites of various kinds, whether from GMC or Toyota or a comparison shopping site. . . . Conversely, all three of the African-American names yielded at least one ad related to bad credit card loans and included other ads related to non-new car purchases."[117]

A Google spokesperson blamed "flawed methodology" for Newman's "wildly inaccurate conclusion," and claimed that Google would never "select ads based on sensitive information, including ethnic inferences from names."[118] The black box nature of reputation algorithms once again defeats any definitive resolution of the issue. Even if we could audit a company to assure ourselves that *intentional* discrimination is not affecting its methods, algorithmic negligence would remain a real concern.[119] It does not take an "ethnic inference" for an algorithm to start tracking "Latanyas" into one set of online opportunities and "Tanyas" into another. It could simply happen as a mechanical extrapolation of past evaluations of people with either of these names or similar ones. Without access to the underlying data and code, we will never know what type of tracking is occurring, and how the discrimination problems long documented in "real life" may even now be insinuating themselves into cyberspace.[120] As FTC chair Edith Ramirez has argued, we must "ensure that by using big data algorithms [firms] are not accidentally classifying people based on categories that society has decided—by law or ethics—not to use, such as race, ethnic background, gender, and sexual orientation."[121]

Collateral Consequences: The problem of collateral consequences is well known in the criminal justice system. Once someone has been convicted of a crime (or pleaded guilty), that stigma will often preclude him from many opportunities—a job, housing, public assistance, and so on—long after he has "paid his debt to society."[122] A similar dynamic is becoming apparent in finance. As they dole out opportunities for "prime" and "subprime" credit, automated systems may be silently resegregating racial groups in ways that would be clearly illegal if pursued consciously by an individual.[123]

"Data-driven" lending practices have hit minority communities hard. One attorney at the Neighborhood Economic Development Advocacy Project (now the New Economy Project) called subprime lending a systematic "equity stripping" targeted at minorities—even if they were longtime homeowners.[124] Subtle but persistent racism, arising out of implicit bias or other factors, may have influenced *past* terms of credit, and it's much harder to keep up on a loan at 15 percent interest than one at 5 percent.[125] Late payments will be more likely, and then will be fed into *present* credit scoring models as *neutral*, *objective*, *nonracial* indicia of reliability and creditworthiness.[126] Far from liberating individuals to be judged on their character rather than their color, credit scores in scenarios like these launder past practices of discrimination into a black-boxed score, immune from scrutiny.[127]

Continuing unease about black box scoring reflects long-standing anxiety about misapplications of natural science methods to the social realm.[128] A civil engineer might use data from a thousand bridges to estimate which one might next collapse; now financial engineers scrutinize millions of transactions to predict consumer defaults. But unlike the engineer, whose studies do nothing to the bridges she examines, a credit scoring system *increases the chance* of a consumer defaulting once it labels him a risk and prices a loan accordingly. Moreover, the "science" of secret scoring does not adopt a key safeguard of the scientific method: publicly testable generalizations and observations.[129] As long as the analytics are secret, they will remain an opaque and troubling form of social sorting.

Bias can embed itself in other self-reinforcing cycles based on ostensibly "objective" data. Police in the past may have watched certain

neighborhoods more closely than others. Thus it's not surprising if such neighborhoods account for a disproportionate share of the overall number of crimes recorded, *even if crime rates are identical across neighborhoods*, because they happen to be where the police were looking. Once that set of "objective" data justifies even more intense scrutiny of the "high crime" neighborhoods, that will probably lead to more arrests—perhaps because of a real crime problem, but perhaps instead due to arrest quotas or escalating adversarialism between law enforcement and community members.[130] The *reasons* for data like arrest numbers matter.

In contexts like policing, there is often no such thing as "brute data," objective measures of behavior divorced from social context or the biases of observers.[131] When there is documented disparate impact in policing practices, the data gathered by law enforcers are scarcely a font of objective assessments of criminality.[132] Drug or gun possession is as likely among whites as it is among racial minorities, but in New York City, racial minorities comprise the vast majority of persons who are "stopped and frisked."[133] Disproportionately more nonwhites than whites, therefore, will end up with criminal records for gun or drug possession. That is one reason that ten states and fifty-one cities prohibit many employers from inquiring into job applicants' criminal histories.[134] But how many other suspect "data points" are silently working their way into automated decision making?

The Birth of a Surveillance Nation

When the government gets into the reputation game, the stakes get very high very fast. It's not just that private corporations are using government records, like arrests, to make decisions. Police and intelligence agencies are using their databases, and private records, to revolutionize their own role in society.[135] The dark axiom of the NSA era says that you don't have to worry if you have nothing to hide. But if your political activities or interests deviate even slightly out of the mainstream, you do.[136]

In 2007, officers arrested law student and journalist Ken Krayeske while he took pictures of the Connecticut gubernatorial parade. He was identified as a potential threat on the basis of blog posts in

which he encouraged protests of the governor's inaugural ball, his service as a Green Party candidate's campaign manager, and one arrest for a misdemeanor at an antiwar rally. He spent thirteen hours in jail before prosecutors dropped the charges.[137]

In Maryland, fifty-three antiwar activists, including two nuns and a Democratic candidate for local office, were placed on terrorist watch lists.[138] The false classification was shared with federal drug enforcement and terrorist databases, as well as with the NSA.[139] Like those wrongly tagged with wrongdoing by commercial data brokers, these victims will have to work hard to clear their names. And the hurdles will likely be more daunting. The post-9/11 "information-sharing environment (ISE)," as the government calls it, means that there are too many databases of suspicion even to know where to start.

In 2010, the ACLU published a report called "Policing Free Speech." It lists incidents in which police spied on Americans, or infiltrated their organizations, "for deciding to organize, march, protest, espouse unusual viewpoints, and engage in normal, innocuous behaviors such as writing notes or taking photographs in public." The Americans spied on included Quakers, vegans, animal activists, Muslims, and an individual who was handing out pamphlets critical of the FBI.[140]

We all know by now that the government has been taking a very keen interest in cultivating "intelligence" about its citizens.[141] There has been a world of outrage both over the NSA's overreach and the fact that it's gotten away with it. But I won't add to that here. My point is narrower: that the government's interest in intelligence gathering has led it into a pragmatic, powerful, and largely secret partnership with interests whose concern is not the public good, but private profit or personal advance.

The most visible and controversial example so far has been the cooperation in Manhattan between the Department of Homeland Security, the New York Police Department, and several major banks.[142] By 2009, the Lower Manhattan Security Coordination Center (LMSCC) was processing feeds from thousands of cameras run by Wall Street firms and the NYPD. One source identified Goldman Sachs, Citigroup, the Federal Reserve, and the New York

Stock Exchange as participants at the center. The exact composition of the staff is a closely guarded secret, but there are likely many other Wall Street firms with "on-site representatives."[143]

In the abstract, a post-9/11 partnership of this sort might seem like an efficient use of resources. But critics worried it would focus on protests like Occupy Wall Street, which was the target of other unusual federal involvements.[144] Homeland Security officials may have advised local police about others of the hundreds of Occupy encampments that arose in the fall of 2011.[145] According to documents obtained by the Partnership for Civil Justice, the Domestic Security Alliance Council described a "strategic partnership between the FBI, the Department of Homeland Security and the private sector" to closely monitor Occupy protests. Educational institutions were deputized by the Feds to spy on sympathetic members of their own communities; the FBI in Albany and the Syracuse Joint Terrorism Task Force sent information to campus police officials at SUNY–Oswego and followed the activity of students and professors there.[146]

What was actually happening in the Occupy villages to merit all this spying? Well, a golden calf was carried around. (It was later taken to Washington by a group called Catholics United, who petitioned House Speaker John Boehner to support a tax on financial transactions.) A debt jubilee was proposed to redress decades of rising inequality. Activists decried bank crimes and outsized bonuses. Yes, there were some confrontations (many of them initiated by police). But Occupy was an essentially peaceful protest, exemplifying freedoms specifically singled out by the First Amendment for protection.[147]

That being so, we can certainly ask whether the federal government should have been gathering intelligence on it at all. There's a more pointed question, though: Once it *did* get involved, should it have been partnering with banks whose managers made millions of dollars during the financial crisis of 2008 on the basis of ethically and legally dubious practices?[148] Even while Occupy was denouncing the failure of the Department of Justice and the FBI to prosecute the banks' lawbreaking, the Bank Fraud Working Group of the FBI's Denver field office "met and were briefed on Occupy Wall

Street in November 2011."[149] In its funding of the LMSCC, the government made Occupy's case for it by enacting the very corporate-state collusion that Occupy was protesting. How else, one indignant observer wanted to know, can we explain "$150 million of taxpayer money going to equip a government facility in lower Manhattan where Wall Street firms, serially charged with corruption, get to sit alongside the New York Police Department and spy on law abiding citizens"?[150]

An "Information-Sharing Environment." But for all its drama, Occupy was just one small corner of a very large picture. After 9/11, the government moved quickly to improve its surveillance capacities by establishing what it called an "information-sharing environment," or ISE. Out of this effort came two collaborative programs that I'll discuss here. One was called Virtual USA, "a pilot information-sharing initiative under the Department of Homeland Security . . . intended to facilitate disaster response by sharing technology, information, and data across federal, state, and local jurisdictions."[151] The other was the establishment of the *fusion centers*, which the Department of Homeland Security describes as "collaborative effort[s] of two or more agencies . . . with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity." They are regional focal points for gathering and sharing government *and private* information related to "threats."[152] There are over seventy of them now, and with their generous federal funding, slick conferences, and firm corporate backing, they are beginning to unite the public and private monitoring of individual lives into unified digital dossiers.[153] They also keep track of their critics: as the *New York Times* has reported, "people connected to the [fusion] centers shared information about individual activists or supporters [during Occupy protests], and kept track of those who speculated in social media postings that the centers had been involved when police departments used force to clear Occupy camps."[154]

The guiding principle of the fusion centers is "the more information, the better."[155] Where do they get their information? They access public- and private-sector databases of traffic tickets, property records, identity-theft reports, drivers' licenses, immigration records,

tax information, public health data, criminal justice sources, car rentals, credit reports, postal and shipping services, utility bills, gaming, insurance claims, and data-broker dossiers.[156] They monitor nonprofit contributions, political blogs, and home videos.[157] They mine footage from law enforcement, transportation, and corporate security cameras.[158] In Southern Nevada, they check out photos and videos from the local hotels and casinos.[159]

In short, fusion centers allow the government, in the name of "information sharing," to supplement its *constitutionally constrained* data-gathering activities with the *unregulated* collections of private industry. In return, the government amplifies the limited reach of local law enforcement, and sometimes even of private industry, with its greater power and larger scope.

Data Mining and Law Enforcement. Even many civil libertarians would not object to fusion centers if they restricted themselves to the responsible deployment of antiterrorist intelligence. But they do not. The Center for Investigative Reporting notes that "since so many states are unlikely to be struck by terrorists, fusion centers have had to expand their intelligence mission to cover all crimes and potential hazards, partly to convince local legislators they're worth financing with taxpayer money into the future."[160] Pork-barrel politics trumps sensible security policy.

When the Alabama Department of Homeland Security started working on a Virtual Alabama database collaboration with Google Earth, for example, local police departments weren't very supportive.[161] Surveillance researcher Torin Monahan says that the problem was solved when "DHS promised to include a GIS [geospatial information system] overlay for all registered sex offenders in the state, showing exactly where each of them are supposed to be residing."[162] What began as a national homeland security project expanded into state law enforcement. Expansion of the antiterror mission helped generate "buy in" from local and state agencies that did not themselves feel threatened by terrorism.[163] This is a common outcome in many fusion centers.[164]

Thus the combined resources of essentially unregulated industry data collecting, the close surveillance capacities of local law en-

forcement, and the massive power of the federal government are at each other's disposal, and largely free from their own proper constraints. Fusion centers are the door into a world where *all* data sources are open to law enforcement inspection and may be used secretly to generate probable cause for criminal investigation.[165]

The line between military and police action is also breaking down. Consider the following Orwellian collaboration, which Reuters reported in 2013. It began when the NSA gave "tips" (which it could have gotten, as we'll see presently, from absolutely anywhere, including Facebook or Google) to the Special Operations Division (SOD) of the Drug Enforcement Administration (DEA), which in turn gave them to the Internal Revenue Service. The legal status of such information sharing is murky at best; national security data is not supposed to be used for law enforcement purposes. But the SOD apparently sidestepped these niceties by creating criminal investigations in which they *retrospectively fabricated* alternative grounds for suspecting and investigating the targets.[166]

This is a black box arrangement of surpassing and appalling elegance. Separate and parallel "realities" are constructed and documented. One is the secret record of how the targets were actually selected; the other is specially invented for consumption by the courts. Two senior DEA officials defended this program and called it legal, but they disclosed neither their names nor any reasoning to support their contention. Michael Hayden, former head of the NSA and the CIA, has also generally defended these practices without offering any explicit legal arguments to support his position.[167] In the summer of 2013, five senators asked the Department of Justice to assess the legality of "parallel construction"; it has yet to respond.[168]

Traditionally, a critical distinction has been made between *intelligence* and *investigation*. Once reserved primarily for overseas spy operations, "intelligence" work is anticipatory; it is the job of agencies like the CIA, which gather potentially useful information on *external* enemies that pose threats to national security. "Investigation" is what police do *once they have evidence of a crime*. But the boundaries between the two are blurring.

This is another black box. State and federal law enforcement rarely shared information or intelligence before 9/11,[169] but since

then, Congress has allocated over $500 million in grants to fusion centers to encourage such collaboration.[170] What police force wouldn't want such expanded powers? The possibility of preemptive "intelligence-led policing" (as opposed to the reactive after-the-fact sort) is tempting indeed.[171]

However, the sweeping techniques of post-9/11 surveillance and data gathering are of a scale appropriate to wholesale calamities like terror attacks and natural disasters, not to ordinary crime or protest. Thousands of people are being caught in data-driven dragnets for being activists, or just belonging to a suspect "identity" group.[172] Careful protection of the boundary between crime and dissent is not a high priority of the intelligence apparatus. One state official commented, "You can make an easy kind of a link that, if you have a protest group protesting a war where the cause that's being fought against is international terrorism, you might have terrorism at that protest. You can almost argue that a *protest* against [the war] is a *terrorist* act."[173] It would be nice to be able to dismiss this statement as an outlier, but FBI director Robert Mueller legitimized it all the way back in 2002, warning that "there is a continuum between those who would express dissent and those who would do a terrorist act."[174] That is a frightening expansion of the "threat matrix."

If mistakes were rare, we'd have less cause for worry. But a critical mass of civil liberties concerns is accumulating. The Virginia Fusion Center's *2009 Virginia Terrorism Threat Assessment Report* urged that student groups be monitored on the grounds that they "are recognized as a radicalization node for almost every type of extremist group."[175] The Missouri Information Analysis Center's 2009 report to highway officers suggested that "violent extremists" typically associate with third-party candidates such as Ron Paul and Bob Barr, and that "potential threats" include anti-immigration and antitax advocates.[176] According to that report, violent extremists could also be identified by bumper stickers on their cars indicating support for libertarian groups.[177]

The Fading Divide between "State" and "Market"

The mountains of data collected by private corporations make them valuable partners in "information sharing." There's plenty of room

for dealing on both sides. Government agencies want data that they can't legally or constitutionally collect for themselves; data brokers have it and want to sell it.[178] Other kinds of companies can make other kinds of trades.[179]

For example, Daniel Solove documents a post-9/11 information exchange that confounds conventional distinctions between "market" and "state": "In violation of its [own] privacy policy, JetBlue Airlines shared the personal data of 1 million customers with Torch Concepts, an Alabama company contracting with the Defense Department to profile passengers for security risks. Torch combined the JetBlue data with SSNs, employment information, and other details obtained from Acxiom, Inc., a database marketing company."[180] While all these entities deserve the tools they need to deflect real terror threats, have they done enough to secure the data from hacks and other security threats? We may never know, given the veil of secrecy draped around "homeland security" matters.

Businesses may support the intelligence apparatus simply to gain a competitive edge. For example, in Washington, Boeing has enjoyed "real-time access to information from the fusion centers" thanks to its participation in the Washington Joint Analytical Center (WJAC).[181] According to a Boeing executive, the company hopes "to set an example of how private owners of critical infrastructure can get involved in such centers to generate and receive criminal and anti-terrorism intelligence." Starbucks, Amazon, and Alaska Airlines have expressed interest in placing analysts at the WJAC.[182]

After FedEx's CEO announced that his company would cooperate with the government, FedEx received a range of government perks including special access to government security databases, a seat on the FBI's regional terrorism task force—where it was the only private company so represented—and an exceptional license from the state of Tennessee to develop an internal police force.[183] Like the banks integrated into the Lower Manhattan setup, FedEx is sharing the privileges and immunities of the state, but not the accountability.

Google is also reported to have entered into deals with the NSA, but an effort by the Electronic Privacy Information Center (EPIC) to find out whether that was indeed the case was quashed by a federal

judge.[184] The NSA neither confirms nor denies working with Google to develop its intelligence operations, even after the spectacular revelations of Edward Snowden in 2013.

Armies and spies have always relied on stealth; after all, loose lips sink ships. But secrecy also breeds conflicts of interest. Why should Google worry about potential antitrust violations if it's monitoring Internet access side by side with the DHS and the NSA?[185] Like the "too big to fail" banks, it may be "too important to surveillance" for the government to alienate the firm. In 2013, in fact, leaked documents showed that the NSA (or a British partner) targeted the official who was in charge of investigating Google's alleged violations of EU competition law.[186] As a growing literature suggests, privatization can be more than a transaction between government and business. It can be a marriage—a secret marriage—with a hidden economy of favors exchanged.[187]

Revolving-door issues loom especially large; government officials looking out for their futures may channel work to a company or industry they have their eyes on.[188] Many security officials go on to lucrative private-sector employment soon after leaving public service.[189] The manipulation of threat perception by the "homeland security-industrial complex" feeds corporate profits as well as government budgets.

All Threats, All Hazards, All Information?

Though critics like James Bamford and Tim Shorrock have thoughtfully covered the intelligence beat for years, the full extent of the government's independent data-gathering practices exploded into public awareness in 2013, when NSA contractor Edward Snowden leaked material documenting extensive domestic surveillance. Snowden's files suggest that the NSA is working directly with (or hacking) our largest telecom and Internet companies to store and monitor communications; that the agency can seize and bug computers that have never been attached to the Internet; and that it can crack many types of encryption that had previously been thought secure.[190]

Very little of this relentless collecting is inspired by suspicion about any particular person or plot. It is done routinely, creating an

ever-expanding haystack of stored information that may someday reveal a needle.[191] Not only telecom firms but also the largest Internet companies are either targeted by the NSA, working with it, or engaged in some combination of complicity and resistance. Google, Facebook, and Microsoft show up frequently in the Snowden slides; their data stores were apparently a rich resource for the surveillance state. Laws prevent the government from collecting certain kinds of information on citizens, but data brokers are not so constrained. *And once someone else has collected that information, little stops the government from buying it, demanding it, or even hacking into it.*

Our off- and online actions are logged in hundreds of private-sector databases. Aptly called "big brother's little helpers" by privacy expert Chris Hoofnagle, private-sector data brokers gather files that police would never be able to gather on their own, and then sell them to the police. This is not a "bug" in our surveillance system, but a "feature."[192] Note that the very definition of fusion centers includes their willingness to receive information from private parties. The Snowden leaks make the shared infrastructure of state and private data collection incontrovertible. Never again can data deregulationists claim that corporate data collection is entirely distinct and far less threatening than government surveillance. They are irreversibly intertwined.

Enduring Opacity

Despite the leaks of Snowden (and Chelsea Manning and Julian Assange), the national surveillance apparatus is still opaque on many levels.[193] It enjoys both real and legal secrecy, hidden as it is in secure networks and protected by the heavy hand of the law. There's plenty of complexity, too, should secrecy fail. Intelligence agencies commission private defense contractors like SAIC, Northrop Grumman, Booz Allen, and Palantir to devise specialized software to monitor their data sources—which include social networks.[194] Their algorithms are complex enough by themselves, but the contractors are also bound to protect company trade secrets. Even oversight bodies that might—in principle—investigate purely governmental actions are hampered by a layer of commercial secrecy designed to maintain the value of private-sector spy methodology.

How could a firm exploit the full economic value of its intellectual property if some pesky oversight board (or, God forbid, journalist) could inspect it?

An unaccountable surveillance state may pose a greater threat to liberty than any particular terror threat.[195] It is not a spectacular danger, but rather an erosion of a range of freedoms.[196] Most insidiously, the "watchers" have the power to classify those who dare to point this out as "enemies of the state," themselves in need of scrutiny. That, to me, is the core harm of surveillance: that it freezes into place an inefficient (or worse) politico-economic regime by cowing its critics into silence. Mass surveillance may be doing less to deter destructive acts than it is slowly narrowing of the range of tolerable thought and behavior.

No Exit

National security surveillance and corporate spying don't much resemble each other on the surface; the ostensible purposes, the techniques, and the scope are all very different. The stakes are different, too, at least theoretically. Private companies may object that regulation would reduce their profits, but the state can assert that without "total information awareness" we are all at risk for disastrous attack. In "national security matters," it's very hard to stop the government from doing exactly what it wants, even if what it wants isn't legal. For all these reasons, it can be harder to regulate a surveillance state than a surveillance corporation.

Still, in their black box structure, and in their developing collaboration, the two are more alike than otherwise. There are powerful bosses at the top, managers, analysts, and programmers in the middle, and a vast cast of outsiders watched at will. The same person may spend a few years at a tech firm, then serve in government, and then go back into business. Their activities ultimately raise similar questions. One is about the flow of information: Can we stop pervasive data collection? I think that the answer to that is probably no. The second question, therefore, is, What do we do?

Self-Helpless. Suggestions abound for digital self-protection; they range from the pedestrian to the fantastic, and from the obvious to

the uber-arcane. There are personal security techniques, like strong passwords, restrictive privacy settings, "burner" phones, and vetting our online presence. Schools have begun to teach the basics of "cyberhygiene," a kind of preventive care for the digital self.[197] Not enough? The Electronic Frontier Foundation pushes for strong encryption. The Electronic Privacy Information Center wants web browsers to default to "do not track." Professor Helen Nissenbaum at NYU looks to creative obfuscation: her browser extension *TrackMeNot* floods your search engine with so many random queries that companies like Google can't compile an accurate psychological or marketing profile.[198] Presumably the same technology could be applied to Gmail by sending dozens of fake e-mails to dummy accounts. Other apps offer to watch our backs and tell us exactly who is sharing our data with others, and how.[199] There are "personal data vaults" in which we can store our information securely and then bargain, one-on-one, with anyone who wants access to it.[200]

But self-help can take us only so far. For nearly every "Privacy Enhancing Technology" (PET) developed, a "Privacy Eviscerating Technology" may arise. Week by week the PET recommendations of digital gurus are rendered obsolete by countermeasures. The best personal security in the world is nothing to a hacker with direct access to an account.[201] Huge databases of usernames, credit card numbers, and social security numbers already exist online, out of which a query as simple as "filetype:xls site:ru login" on a search engine will realize millions of passwords.[202] (*But before you try this, note that the search may be logged to your IP address and might tag you as a possible crook.*) We've talked about the gigabytes of sensitive consumer data that Target lost to hackers. The health care sector hosts a "Wall of Shame" that lists hundreds of data breaches.[203]

On social networks especially, cyberhygiene may be an exercise in futility. These sites have been known to change their default privacy settings without warning, opening "private" communications to general inspection. What if, as many states allow, a prospective employer asks for the password to your Facebook account? Give it, and you're exposed. Refuse, and you may have lost your chance at the job.[204] And let's say you actually do manage to track down an online calumny. In the United States, Google won't remove it from

the sites it serves up when someone searches for your name; it just refers you to the sites themselves.[205] Unless you can prove falsehood in a court of law (or hire a "reputation manager" to drive the offending sites down in Google rankings), you're probably out of luck.

Furthermore, attempts to foil known privacy vulnerabilities and reputational threats can open up new ones. It would be nice to think that the "private browsing" setting will keep our Internet habits secret. But our ISPs, the websites we visit, and the ad networks present there all may be keeping track of our computers' unique IP addresses. The anonymization tool Tor, recommended by tech-savvy journalists to hide digital identities, may have been compromised. Even if it hasn't been, the very fact of using it may invite suspicion and closer surveillance. As soon as an encryption program gets too popular, it provokes rumors that it is a kind of honeypot, a promise of privacy that lures people into spilling their secrets in (what turns out to be) an intensively monitored environment.[206]

It's an endless cycle. When "device fingerprinters" begin to identify our computers and cell phones, journalists offer advice about masking their data trail. But even the scholars of surveillance have a tough time keeping up with all the new threats; the *Wall Street Journal*'s "What They Know" series has tracked dozens of privacy-diminishing technologies developed since 2010.[207] One thing is certain: "self-help" as a solution here fails on practical grounds for all but the most skilled (or wealthy) Internet users, and thus fails on moral grounds as well. A technological arms race will quickly leave most users behind.

Even nascent legal solutions may only delay, rather than deflect, invasive surveillance. For example, at least fourteen states have banned employers from requesting social network account passwords from current workers or applicants.[208] But what if competitive applicants start volunteering them? They may leave the privacy-concerned behind, regardless of their formal legal rights. Economists of information label this process "unraveling," and even well-intentioned protections are undermined by it.[209] Offering a password on an application may now seem like a desperate effort to stand out from the crowd. But the many people who make their posts "public" (rather than "friends only") are offering much of the

information the password would grant. Where is the tipping point between "competitive advantage" and "what everybody does"? Until the *use* of sensitive information is prohibited (and audited), a full-disclosure future is foreordained.[210]

A One-Percent Solution. Contracting out reputation management to a private company is a growing "market solution" to the emerging traffic in data. Our brave new digital world is a much safer place for those with the time and money to hire lawyers to review terms of service, programmers to install layers of encryption on their computing systems, and reputation managers to tend to their online profiles. And it's a very lucrative place for those who can supply those services. Firms are already trading on the mysteries of Google rankings to nurture their clients' images online. It's only a matter of time before they extend their services to those looking to optimize the impressions they make on other data gatherers.

But is this how we want to handle the problem of invasive data collection? It hasn't worked well in the world of financial privacy.[211] Yes, with enough legal and accounting help, very wealthy people can hide their money from the taxman. But only the richest have the resources and time to develop foolproof versions of their own, personal black boxes. And the costs are very high to the global economy. Using multiple estimation methods, James Henry, a senior adviser to the Tax Justice Network, calculated the total amount of money hidden away from tax authorities as between $21 and $32 trillion.[212]

A report titled "Secrecy for Sale: Inside the Offshore Money Maze" reveals many of the grim details.[213] The techniques described work well for the possessors of investment income, who may well wish to extend them to their reputational affairs, adding a division of "reputation defense" to the wealth defense industry. But this Swiss Bank model would only entrench the divide between haves and have-nots. It will do more to stratify privacy protections than to guarantee them. It does not address the real problems of invasive data collection or unfair data use.

Full-Disclosure Future

Even if absolute secrecy could somehow be democratized with a universally available cheap encryption tool, would we really want it? I don't think I want the NSA blinded to real terrorist plots. If someone developed a fleet of poison-dart drones, I'd want the authorities to know. I wouldn't want so-called "cryptocurrencies" hiding ever more money from the tax authorities and further undermining public finances.[214] Biosurveillance helps public health authorities spot emerging epidemics. Monitoring helps us understand the flow of traffic, energy, food, and medicines.[215]

So while hiding—the temptingly symmetrical solution to surveillance—may be alluring on the surface, it's not a good bet. The ability to hide—and to detect the hiders—is so comprehensively commodified that only the rich and connected can win that game. The help and the harm of information collection lies not in the information itself but in how it is used. The decisions we make about that have plenty to tell us about our priorities.

The digital economy of the moment prioritizes marketing over productivity. It's less likely to reward the builder of a better mousetrap than to fund start-ups that identify people likely to buy one. The critical point is no longer the trap or even the rodents, but the data: the constant streams of numbers that feed algorithmic systems of prediction and control. Profiling is big business in an economy like that. Cyberlibertarians used to brag that the Internet "reads censorship as damage and routes around it"; replace "censorship" with "privacy" and the statement would be just about as true.[216]

Much of the writing about the scored world focuses on how to outwit the evaluators—how to get an 800 credit score, how to "ace" job personality tests. But this vast and growing literature ignores the possibility of criticism, much less resistance. Economic models of the data can be even worse, complacently characterizing personalization as a mere matching problem (of, say, the riskiest borrowers to the highest interest rate loans). From a legal perspective, things can look very different: myriad penalties are imposed without even a semblance of due process.

If we're not going to be able to stop the flow of data, therefore, we need to become more knowledgeable about the entities behind it and learn to control their use of it. We need to hold business and government to the same standard of openness that they impose upon us—and complement their scrutiny with new forms of accountability. We need to enforce the laws that define fair and unfair uses of information. We need to equalize the surveillance that is now being aimed disproportionately at the vulnerable and ensure as best we can that critical decisions are made in fair and nondiscriminatory ways. We need to interrupt the relentless cascades of judgment that can turn one or two mistakes into a self-fulfilling prophecy of recurrent failure. And we need to plan for the inevitability that as soon as we open one black box, new modes of opacity will arise.

Thomas Jefferson once said that "he who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me."[217] To many of us this is an inspiring vision. But the total information dominance to which America's defense, police, and corporate institutions now aspire reflects a diametrically opposed mind-set. The black box society is animated by the belief that information is useful only to the extent that it is exclusive—that is, secret. Terrorists have to be kept in the dark because they're dangerous. Sick people have to be kept in the dark because they're expensive. To faceless algorithms, we might be terrorists, or sick. So we are kept in the dark, too.

It is time to reclaim our right to the presumption of innocence, and to the security of the light. It may be that we cannot stop the collection of information, but we can regulate how it is used. This is easier said than done; data collection has run so wild that it will take time and effort to purify reputation systems of inaccurate or unfair data points. But the alternative is worse. One of the best-known privacy blogs is entitled "Pogo Was Right," in honor of the old comic book tag "We have met the enemy, and he is us." The rebuke is obvious: we'd better stop being so careless about how technology creates reputations, and start to rein in arbitrary, discriminatory, and unfair algorithms. Chapter 5 suggests some initiatives for achieving

that end. But to fully understand how they might work, and how needed they are, we need to turn from technologies of reputation (which increasingly mediate how we *are perceived*), to technologies of search (which mediate how *we perceive*). Search is the topic of the next chapter.

NOTES

Book Epigraphs

Heracleitus, *On the Universe*, in *Hippocrates IV*, Loeb Classical Library 150, trans. W. H. S. Jones (Cambridge: Harvard University Press, 1931), 501.

Gerald Manley Hopkins, "That Nature is a Heraclitean Fire and of the Comfort of the Resurrection." *Poetry Foundation*. Available at http://www.poetryfoundation.org/poem/173662.

1

Introduction—The Need to Know

1. Harold D. Lasswell, *Politics: Who Gets What, When, How* (New York: Meridian Books, 1972).

2. Robert H. Frank and Philip J. Cook, *The Winner-Take-All Society* (New York: Penguin, 1996); David C. McClelland, *The Achieving Society* (Eastford, CT: Martino Fine Books, 2010); Hassan Masum and Mark Tovey, eds., *The Reputation Society* (Cambridge, MA: MIT Press, 2012); Jeffrey M. Berry and Clyde Wilcox, *The Interest Group Society* (Upper Saddle River, NJ: Pearson, 2008); Robert N. Bellah et al., *The Good Society* (New York: Vintage, 1992); Avishai Margalit, *The Decent Society* (Cambridge: Harvard University Press, 1996). Critiques of social order can also take this form; see, e.g., Robert B. Edgerton, *Sick Societies* (New York: Free Press, 1992).

3. Gillian Tett has described "social silences" at the core of the economy. Gillian Tett, *Fool's Gold* (New York: Free Press, 2009). Sociologist John Gaventa has focused on what is kept *off* political agendas as a "third dimension" of power, building on Antonio Gramsci's theories. John Gaventa, *Power and Powerlessness* (Champaign: University of Illinois Press, 1982). David E. Pozen, "Deep Secrecy," *Stanford Law Review* 62 (2010) 257–340.

4. Robert N. Proctor, "Agnotology: A Missing Term to Describe the Cultural Production of Ignorance (and Its Study)," in *Agnotology: The Making and Unmaking of Ignorance*, ed. Robert N. Proctor and Londa N. Schiebinger (Stanford, CA: Stanford University Press, 2008), 3.

5. Alan Greenspan, "Dodd-Frank Fails to Meet Test of Our Times," *Financial Times*, March 29, 2011; Friedrich A. Hayek, "The Use of Knowledge in Society," *American Economics Review* 35 (1945): 519–530. Of course, as Richard Bronk observes, "Hayek's analysis falls short by ignoring the role of dominant narratives, analytical monocultures, self-reinforcing emotions, feedback loops, information asymmetries and market power in distorting the wisdom of prices." Richard Bronk, "Hayek on the Wisdom of Prices: A Reassessment," *Erasmus Journal for Philosophy and Economics* 6, no. 1 (2013): 82–107.

6. Lee H. Fang, "The Invisible Hand of Business in the 2012 Election," *The Nation*, November 19, 2003, http://www.thenation.com/article/177252/invisible-hand-business-2012-election.

7. In philosophy, the term is also polysemic. For example, if enough people simply accept the outputs of a given process as valid, *it* is a quite useful black box. Some aspects of reality are simply assumed to be true, without need for further investigation. Graham Harman stated, "We have a true black box when a statement is simply presented as raw fact without any reference to its genesis or even its author. As Latour asks, 'who refers to Lavoisier's paper when writing the formula H_2O for water?' " Harman, *Prince of Networks: Bruno Latour and Metaphysics* (Melbourne: re.press, 2009), 37. One of the main purposes of this book is to raise enough questions about the results presented by leading Internet and finance firms so that they do not congeal into this kind of black box.

8. Jack Balkin, "The Constitution in the National Surveillance State," *Minnesota Law Review* 93 (2008): 1–25.

9. George Packer, "Amazon and the Perils of Non-disclosure," *The New Yorker*, February 12, 2014.

10. Arkady Zaslavsky, "Internet of Things and Ubiquitous Sensing" (Sept. 2013). *Computing Now*. Available at http://www.computer.org/portal/web/computingnow/archive/september2013.

11. April Dembosky, "Invasion of the Body Hackers," *Financial Times*, June 10, 2011.

12. Tal Zarsky, "Transparent Predictions," *Illinois Law Review* (2013): 1503–1570.

13. Bradley Keoun and Phil Kuntz, "Wall Street Aristocracy Got $1.2 Trillion in Secret Loans," *Bloomberg News*, August 22, 2011, http://www.bloomberg.com/news/2011-08-21/wall-street-aristocracy-got-1-2-trillion-in-fed-s-secret-loans.html.

14. Maxwell Strachan, "Financial Sector Back to Accounting for Nearly One-Third of U.S. Profits," *Huffington Post* (blog), March 30, 2011, http://www.huffingtonpost.com/2011/03/30/financial-profits-percentage_n_841716.html. Things were even better for the finance firms in the boom years.

15. Jaron Lanier, *Who Owns the Future?* (New York: Simon & Schuster, 2013). "At the height of its power, the photography company Kodak employed

more than 140,000 people and was worth $28 billion. They even invented the first digital camera. But today Kodak is bankrupt, and the new face of digital photography has become Instagram. When Instagram was sold to Facebook for a billion dollars in 2012, it employed only thirteen people." Ibid., 2.

16. Frederic Bloom, "Information Lost and Found," *California Law Review* 100 (2012): 635–690.

17. Obfuscation contributes to *complexity*, which is sometimes the natural result of modern business, but it is also, frequently, contrived for no good end. Steve Randy Waldman, "Why Is Finance So Complex?" *Interfluidity* (blog), December 26, 2011, http://www.interfluidity.com/v2/2669.html.

18. As G.K. Chesterton observed, the irremediably unknown is a mystery. We cannot solve or dissect it, but only grow wiser about it.

19. This is an old problem in law. See Grant Gilmore, "Circular Priority Systems," *Yale Law Journal* 71 (1961): 53–74.

20. Frank Partnoy and Jesse Eisinger, "What's Inside America's Banks?," *The Atlantic*, January 2, 2013.

21. Ibid.

22. Clay Shirky, "A Speculative Post on the Idea of Algorithmic Authority," *Shirky* (blog), November 13, 2009, http://www.shirky.com/weblog/2009/11/a-speculative-post-on-the-idea-of-algorithmic-authority/.

23. See Scott Patterson, *The Quants: How a New Breed of Math Whizzes Conquered Wall Street and Nearly Destroyed It* (New York: Crown Publishing, 2010).

24. Jeff Connaughton, *The Payoff: Why Wall Street Always Wins* (Westport, CT: Prospecta Press, 2013). Chapter 10 of Connaughton's book is titled "The Blob," referring to the shadowy exchange of favors among government, lobbyists, businesses, and media interests. For a theoretical and critical take on the intermixture of political and economic elites, see Hanna Fenichel Pitkin, *Attack of the Blob: Hannah Arendt's Concept of the Social* (Chicago: University of Chicago Press, 2000), 5; Janine R. Wedel, *Shadow Elite: How the World's New Power Brokers Undermine Democracy, Government, and the Free Market* (New York: Basic Books, 2009).

25. Jon Elster, *Local Justice: How Institutions Allocate Scarce Goods and Necessary Burdens* (New York: Russell Sage Foundation, 1993).

26. For an insightful account of modeling as rationalization, see Gerd Gigerenzer, *Risk Savvy: How to Make Good Decisions* (New York: Viking, 2014).

27. Ben Goldacre, *Bad Pharma: How Drug Companies Mislead Doctors and Harm Patients* (London: Fourth Estate, 2012), 3; Frank Pasquale, "Grand Bargains for Big Data: The Emerging Law of Health Care Information," *Maryland Law Review* 72 (2013): 668–772 (collecting studies on secrecy in the health context).

28. See, e.g., David Dayen, "Massive new fraud coverup: How banks are pillaging homes — while the government watches," *Salon*, at http://www.salon.com/2014/04/23/massive_new_fraud_coverup_how_banks_are_pillaging_homes_while_the_government_watches/ (Apr. 23, 2014); Yves Smith, "The Private Equity Limited Partnership Agreement Release: The Industry's Snowden Moment, Naked Capitalism," May 28, 2014, at http://www.nakedcapitalism

.com/2014/05/private-equity-limited-partnership-agreement-release-industrys-snowden-moment.html.

29. Dave Gilson, Gavin Aronsen, Tasneem Raja, Ben Breedlove, and E.J. Fox, "An Interactive Map of the Dark-Money Universe" (June 2012). *Mother Jones.* Available at http://www.motherjones.com/politics/2012/06/interactive-chart-super-pac-election-money; Ciara Torres-Spelliscy, "Transparent Elections after Citizens United" (Mar. 2011). *Brennan Center for Justice, New York University School of Law*. Available at https://www.brennancenter.org/publication/transparent-elections-after-citizens-united.

During the debate on the Affordable Care Act, health insurers "publicly stake[d] out a pro-reform position while privately funding the leading anti-reform lobbying group in Washington." Elahe Izadi, "Exclusive: AHIP Gave More than $100 Million to Chamber's Efforts to Derail Health Care Reform," *National Journal* (blog), June 13, 2012, http://www.nationaljournal.com/blogs/influencealley/2012/06/exclusive-ahip-gave-more-than-100-million-to-chamber-s-efforts-to-derail-health-care-reform-13.

30. Shane Richmond, "Eric Schmidt: Google Gets Close to the 'Creepy Line,'" *The Telegraph*, October 5, 2010.

31. Magazines like *McClure's* paved the way for muckrakers and reformers like Brandeis. Adam Curtis, "What the Fluck?" *BBC Blog*, December 5, 2013, http://www.bbc.co.uk/blogs/adamcurtis/posts/WHAT-THE-FLUCK. Curtis also observes the need for such exposure and explanation in our day, explaining that scandals "range from the NSA [U.S. National Security Agency] and GCHQ [Britain's Government Communications Headquarters], to global banks, private equity . . . and parts of the media-industrial complex. . . . But the scandals do not join up to make a bigger picture. And our reactions are sometimes confused and contradictory—as in the case of transparency and surveillance. It is as if the scandals are part of a giant jigsaw puzzle—and what we are waiting for is someone to come along and click those pieces together to give a clear, big picture of what is happening." Ibid.

32. Robert H. Wiebe, *The Search for Order: 1870–1922* (New York: Farrar, Straus and Giroux, 1967), 132. ("They had enough insight into their lives to recognize that the old ways and old values would no longer suffice.")

33. See Trevor Potter and Bryson B. Morgan, "The History of Undisclosed Spending in U.S. Elections and How 2012 Became the Dark Money Election," *Notre Dame Journal of Law, Ethics and Public Policy* 27 (2013): 383–480.

34. The FCC was created by the Communications Act of 1934 (47 U.S.C. § 151 et seq.).

35. Robert L. Rabin, "Federal Regulation in Historical Perspective," *Stanford Law Review* 38 (1986): 1189–1326.

36. Martin Shapiro, "APA: Past, Present, Future," *Virginia Law Review* 72 (1986): 447–492.

37. Harvey J. Goldschmid, ed., Business Disclosure: Government's Need to Know (New York: McGraw-Hill, 1979); President John F. Kennedy, "Secrecy Is Repugnant," YouTube video, 5:29, from an address to newspaper publishers at the Waldorf-Astoria in New York City, April 27, 1961 (posted Dec.

2010). *4TheRecord*. Available at http://tzimnewman.blogspot.com/2010/12/jfk-secrecy-is-repugnant-1961-speech.html. ("The very word "secrecy" is repugnant in a free and open society; and we are as a people inherently and historically opposed to secret societies, to secret oaths and secret proceedings.")

38. Rabin, "Federal Regulation in Historical Perspective."

39. Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984); Pamela Samuelson, "Information as Property: Do *Ruckelshaus* and *Carpenter* Signal a Changing Direction in Intellectual Property Law?," *Catholic University Law Review* 38 (1989): 365–400.

40. For background on (and critique of) the role of the "sophisticated investor" construct in finance theory, see Jennifer Taub, "The Sophisticated Investor and the Global Financial Crisis," in *Corporate Governance Failures: The Role of Institutional Investors in the Global Financial Crisis*, ed. James P. Hawley, Shyam J. Kamath, and Andrew T. Williams (Philadelphia: University of Pennsylvania Press, 2011), 191. (reliance "upon the sophisticated investor ignores reality; the entities the law deems to meet the definition are largely neither sophisticated enough to match the complexity of the instruments or lack of data nor [are they] the actual investors who have placed their capital at risk.")

41. Rakesh Khurana, *From Higher Aims to Hired Hands: The Social Transformation of American Business Schools and the Unfulfilled Promise of Management as a Profession* (Princeton: Princeton University Press, 2009); George F. DeMartino, *The Economist's Oath: On the Need for and Content of Professional Economic Ethics* (Oxford, UK: Oxford University Press, 2011); Charles Ferguson, "Larry Summers and the Subversion of Economics," *The Chronicle Review*, October 3, 2010; Philip Mirowski and Esther-Mirjam Sent, eds., *Science Bought and Sold: Essays in the Economics of Science* (Chicago: University of Chicago Press, 2002).

42. See Frederic Filloux, "Google News: The Secret Sauce," *The Guardian*, February 25, 2013.

43. Neoliberalism is a complex set of ideas, perhaps best summarized in Philip Mirowski, *Never Let a Serious Crisis Go to Waste: How Neoliberalism Survived the Financial Meltdown* (London: Verso, 2013), 53–67. For our purposes, the critical tenet of the neoliberal "thought collective" is that "the market (suitably reengineered and promoted) can always provide solutions to problems seemingly caused by the market in the first place." Ibid., 64.

44. Barton Gellman, *Angler: The Cheney Vice Presidency* (New York: Penguin, 2009), 138.

45. For more, see Julian E. Zelizer, *Arsenal of Democracy* (New York: Basic Books, 2010).

46. Dana Priest and William Arkin, *Top Secret America: The Rise of the New American Security State* (New York: Hachette Book Group, 2011).

47. Noah Shachtman, "Pentagon's Black Budget Tops $56 Billion," *Wired*, February 1, 2010, http://www.wired.com/2010/02/pentagons-black-budget-tops-56-billion/.

48. Glenn Reynolds, *An Army of Davids* (Nashville, TN: Thomas Nelson, 2007); David Brin, *The Transparent Society* (Cambridge, MA: Perseus Books, 1998).

49. "2007 Electronic Monitoring and Surveillance Survey" (Feb. 2008). *American Management Association* (press release). Available at http://press.amanet.org/press-releases/177/.

50. Alexander Halavais, *Search Engine Society* (Cambridge, UK: Polity, 2008), 85; see also Adam Raff, "Search, but You May Not Find," *New York Times*, December 28, 2009, A27.

51. For a general overview of online search engines, see Jon Rognerud, *Ultimate Guide to Search Engine Optimization* (Irvine, CA: Entrepreneur Media, 2008).

52. The lack of transparency, or audits, not only provides opportunities for bias or self-serving behavior. It also undermines the validity of the "findings" driving business here. As Tim Harford has observed, "theory-free analysis of mere correlations is inevitably fragile. If you have no idea what is behind a correlation, you have no idea what might cause that correlation to break down." Tim Harford, "Big data: are we making a big mistake?," *Financial Times*, Mar. 28, 2014, at http://www.ft.com/cms/s/2/21a6e7d8-b479-11e3-a09a-00144feabdc0.html#ixzz32xoXh98S.

53. Jamie Court and John Simpson, Letter to Google, October 13, 2008. *Consumer Watchdog*. Available at http://www.consumerwatchdog.org/resources/CWLetterToGoogle10-13-08.pdf.

54. The prescient Helen Nissenbaum warned of "eroding accountability in computerized societies." Helen Nissenbaum, "Accountability in a Computerized Society," *Science & Engineering Ethics* 2(1) (1996).

55. John Gapper, "The Price of Wall Street's Black Box," *Financial Times*, June 22, 2011.

56. George Dyson, *Turing's Cathedral: The Origins of the Digital Universe* (New York: Pantheon, 2012), 308.

57. State officials closely monitor reputational intermediaries, requiring key "doctor rating" sites to disclose the data they use and the way they analyze it. New health privacy regulations have also focused on an "accounting of disclosures" that should help patients understand how data about them is compiled and disseminated.

58. Many legal scholars have grown disillusioned with disclosure as a regulatory strategy. Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton: Princeton University Press, 2014).

59. David Brin, "The Self-Preventing Prophecy: How a Dose of Nightmare Can Help Tame Tomorrow's Perils," in *On Nineteen Eighty-Four: Orwell and Our Future*, ed. Abbott Gleason, Jack Goldsmith, and Martha C. Nussbaum (Princeton, NJ: Princeton University Press, 2005).

60. Benjamin Kunkel, "Dystopia and the End of Politics," *Dissent*, Fall 2008.

61. George Orwell, *1984* (London: Secker and Warburg, 1949); Aldous Huxley, *Brave New World* (London: Chatto & Windus, 1932).

62. *Brazil*, dir. by Terry Gilliam (1985, Universal Studios, DVD).

63. Of course, their very sophistication and precision may make them *more* menacing in some contexts. Julia Angwin, *Dragnet Nation* (New York:

Times Books, 2014). (A whistleblower told her that "the amount of data being assembled by the NSA was 'orders of magnitude' more than the world's most repressive secret police regimes, the Gestapo, the Stasi, and the KGB.")

2

Digital Reputation in an Era of Runaway Data

1. John Gilliom and Torin Monahan, *SuperVision: An Introduction to the Surveillance Society* (Chicago: University of Chicago Press, 2012), 32.

2. Katy Bachman, "Big Data Added $156 Billion in Revenue to Economy Last Year," *AdWeek*, October 14, 2013, http://www.adweek.com/news/technology/big-data-added-156-billion-revenue-economy-last-year-153107 (reporting on industry estimate of "how much of the economy is driven by companies that use consumer-level data to market and retain consumers").

3. Jennifer Valentino-Devries, Jeremy Singer-Vine, and Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information," *Wall Street Journal*, December 24, 2012, http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534.

4. "Facebook Using Offline Purchase History to Target Ads," *RT*, March 27, 2013, http://rt.com/usa/offline-facebook-ads-history-900/.

5. Charles Duhigg, "Bilking the Elderly, with a Corporate Assist" *New York Times*, May 20, 2007, http://www.nytimes.com/2007/05/20/business/20tele.html?pagewanted=all&_r=0.

6. Inside Google, "Liars and Loans: How Deceptive Advertisers Use Google," February 2011. *Consumer Watchdog.* Available at http://www.consumerwatchdog.org/resources/liarsandloanspluso21011.pdf. Nathan Newman, "The Cost of Lost Privacy, Part 3: Google, the Subprime Meltdown and Antitrust Implications," *Huffington Post* (blog), July 15, 2011, http://www.huffingtonpost.com/nathan-newman/the-cost-of-lost-privacy-_3_b_893042.html. Jeff Chester, "Role of Interactive Advertising and the Subprime Scandal: Another Wake-Up Call for FTC," *Digital Destiny* (blog), August 28, 2007, http://centerfordigitaldemocracy.org/jcblog/?p=349.

7. David Anthony Whitaker, "How a Career Con Man Led a Federal Sting that Cost Google $500 Million," *Wired*, May 1, 2013, at http://www.wired.com/2013/05/google-pharma-whitaker-sting/.

8. Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (Washington: FTC, 2014), vii.

9. Joanne Leon, "Husband Internet Searches on Pressure Cooker and Backpack at Work. Law Enforcement Shows Up at House," *DailyKos* (blog), August 1, 2013, http://www.dailykos.com/story/2013/08/01/1228194/-Wife-searches-online-pressure-cookers-husband-a-backpack-Terrorism-task-force-shows-up-at-house. The police say the search terms included "pressure cooker bomb"; Catalano's account only mentions "pressure cookers." Even if it is the former, we should note that Google's autosuggest feature may have automatically entered the word "bomb" after "pressure cooker" while he was

typing—certainly many people would have done the search in the days after the Boston bombing merely to learn just how lethal such an attack could be. The police had no way of knowing whether Catalano had actually typed "bomb" himself, or accidentally clicked on it thanks to Google's increasingly aggressive recommendation engines. See also Philip Bump, "Update: Now We Know Why Googling 'Pressure Cookers' Gets a Visit from the Cops," *The Wire*, August 1, 2013, http://www.thewire.com/national/2013/08/government-knocking-doors-because-google-searches/67864/#.UfqCSAXy7zQ.facebook.

10. Martin Kuhn, *Federal Dataveillance: Implications for Constitutional Privacy Protections* (New York: LFB Scholarly Publishing, 2007), 178.

11. Robert Ellis Smith, *Ben Franklin's Web Site* (New York: Sheridan Books, 2004), 318–320.

12. 15 U.S.C. § 1681 et seq. (2012); Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 2009), 101; 15 U.S.C. § 1681a(f) (2012).

13. See 15 U.S.C. § 1681i (2012).

14. 60 Minutes, "40 Million Mistakes: Is Your Credit Report Accurate?," CBS News, Aug. 25, 2013, transcript at http://www.cbsnews.com/news/40-million-mistakes-is-your-credit-report-accurate-25-08-2013/4/.

15. See Meredith Schramm-Strosser, "The 'Not So' Fair Credit Reporting Act: Federal Preemption, Injunctive Relief, and the Need to Return Remedies for Common Law Defamation to the States," *Duquesne Business Law Journal* 14 (2012): 170–171 (describing a "regulatory scheme that tends to favor the credit reporting industry").

16. FTC, "Marketer of Free Credit Reports Settles FTC Charges," Aug. 16, 2005, at http://www.ftc.gov/news-events/press-releases/2005/08/marketer-free-credit-reports-settles-ftc-charges. The site freecreditreport.com stated "along with your INSTANT credit report, we'll give you 30 FREE days of the Credit Check Monitoring Service at no obligation," not adequately disclosing that "after the free trial period for the credit monitoring service expired, consumers automatically would be charged a $79.95 annual membership, unless they notified the defendant within 30 days to cancel the service." *See also* EPIC Complaint and Request for Injunction, in the Matter of Experian, at http://epic.org/privacy/experian/.

17. Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004). Daniel Solove, "The ChoicePoint Settlement," *Concurring Opinions* (blog), January 30, 2006, http://www.concurringopinions.com/archives/2006/01/the_choicepoint_1.html.

18. See Letter from Chris Jay Hoofnagle et al. to Joel Winston, Federal Trade Commission, December 7, 2004. Electronic Privacy Information Center (EPIC). Available at http://epic.org/privacy/fcra/freereportltr.html.

19. Daniel Solove, "FTC: Letting Experian Keep the Spoils," *Concurring Opinions*, Nov. 13, 2005, at http://www.concurringopinions.com/archives/2005/11/ftc_letting_exp.html.

20. The Fair, Isaac & Co. (now known as FICO) promised scientific methods of ranking creditworthiness. After a slow start, the company grew steadily,

and its scores drive many credit decisions. Martha Poon, "Scorecards as Devices for Consumer Credit: The Case of Fair, Isaac and Company Incorporated," *Sociological Review* 55 (2007): 289; Kenneth G. Gunter, "Computerized Credit Scoring's Effect on the Lending Industry," *North Carolina Banking Institute* 4 (2000): 445; Martha Poon, "Statistically Discriminating without Discrimination" (dissertation chapter, University of California, San Diego, 2012). Available at http://www.ardis-recherche.fr/files/speakers_file_32.pdf. On predicting derogatory events, see "The FICO Score," *The Credit Scoring Site*, http://www.creditscoring.com/creditscore/fico/ (accessed February 16, 2014); Cassandra Jones Havard, "'On The Take': The Black Box of Credit Scoring and Mortgage Discrimination," *Boston University Public Interest Law Journal* 20 (2011): 241–288.

21. Danielle Keats Citron and Frank Pasquale, "The Scored Society," *Washington Law Review* 89 (2014): 10–15.

22. Kevin Simpson, "Insurers' Use of Credit Reports Rankles Many," *Denver Post*, August 20, 2003, A1 ("Credit-scoring has been one of the components responsible for an 'alarming trend' of increased complaints to regulators over the past three years . . ."); see also Equal Employment Opportunity Commission, "EEOC Files Nationwide Hiring Discrimination Lawsuit against Kaplan Higher Education Corp.," December 21, 2010 (news release), http://www.eeoc.gov/eeoc/newsroom/release/12-21-10a.cfm.

23. For an example of weather catastrophe hurting credit scores (and the bureaus' refusal to respond), see Daniel Solove, "Hurricane Katrina and Credit Scores," *Concurring Opinions*, Oct. 10, 2005, at http://www.concurringopinions.com/archives/2005/10/hurricane_katri_1.html; Amy Traub, "Discredited: How Employment Credit Checks Keep Qualified Workers out of a Job," Demos (Feb., 2013), at http://www.demos.org/sites/default/files/publications/Discredited-Demos.pdf.

24. Brenda Reddix-Smalls, "Credit Scoring and Trade Secrecy: An Algorithmic Quagmire," *University of California Davis Business Law Journal* 12 (2011): 87–124; Havard, "On The Take," 248. ("Credit scoring if unchecked is an intrinsic, established form of discrimination very similar to redlining.")

25. For background on foreclosure fraud, see Yves Smith, *Whistleblowers Reveal How Bank of America Defrauded Homeowners and Paid for a Cover Up—All with the Help of 'Regulators'* (2013). Available at http://econ4.org/wp-content/uploads/2013/04/Naked-Capitalism-Whistleblower-Report-on-Bank-of-America-Foreclosure-Reviews-12.pdf.

26. See, e.g., Matthew Hector, "Standing, Securitization, and 'Show Me the Note,'" *Sulaiman Law Group*, http://www.sulaimanlaw.com/Publications/Standing-Securitization-and-Show-Me-The-Note.shtml (accessed February 15, 2014).

27. Jeff Harrington, "2010 Adds Its Own Terminology to Business Lexicon," *Tampa Bay Times*, December 23, 2010, http://www.tampabay.com/news/business/2010-adds-its-own-terminology-to-business-lexicon/1141681. ("Robo-sign[ing involves] a back-office system of quickly signing off on foreclosure documents like affidavits without actually doing what the affidavits say was done.")

28. See DeltaFreq, Comment to Barry Ritholtz on blog post, "Where's the Note? Leads BAC to Ding Credit Score," *The Big Picture* (blog), December 14, 2010, 11:03 a.m., http://www.ritholtz.com/blog/2010/12/note-bac-credit-score/.

29. Ibid.

30. "Credit Checks and Inquiries," *myFICO*, http://www.myfico.com/crediteducation/creditinquiries.aspx (accessed February 16, 2014).

31. Ibid. ("Generally, people with high FICO scores consistently: Pay bills on time . . . keep balances low on credit cards and other revolving credit products . . . [and] apply for and open new credit accounts only as needed.")

32. See, e.g., G. William McDonald, *Owing! 5 Lessons on Surviving Your Debt Living in a Culture of Credit* (Scottsdale, AZ: ACG Press, 2013).

33. myFICO Forums, http://ficoforums.myfico.com/ (accessed February 15, 2014).

34. "Credit Bureaus and Credit Reporting," *USA.Gov*, April 11, 2013, http://www.usa.gov/topics/money/credit/credit-reports/bureaus-scoring.shtml.

35. Carolyn Carter et al., "The Credit Card Market and Regulation: In Need of Repair," *North Carolina Banking Institute* 10 (2006): 41. (Twenty-nine percent have credit scores that differ by at least fifty points between credit bureaus; 50 to 70 percent of credit reports contain inaccurate information.)

36. Robert Pregulman, "Credit Scoring Highly Unfair," *SeattlePI*, January 28, 2002, http://www.seattlepi.com/local/opinion/article/Credit-scoring-highly-unfair-1078615.php. See also Deirdre Cummings, "Testimony in Favor of an Act Banning the Use of Socio-Economic Factors for Insurance Underwriting and Rating of Motor Vehicle Liability Insurance," *MassPirg* (blog), October 18, 2011, http://www.masspirg.org/blogs/blog/map/testimony-favor-act-banning-use-socio-economic-factors-insurance-underwriting.

37. See, e.g., Consumer Reports, "The Secret Score behind Your Auto Insurance," *MSN*, http://editorial.autos.msn.com/article.aspx?cp-documentid=435604 (accessed February 15, 2014) (noting that "insurance scores can penalize consumers who use credit reasonably"). See M. Beddingfield, "How Important Is Your Debt to Limit Ratio?" *Saving Advice*, October 11, 2008, http://www.savingadvice.com/articles/2008/10/11/102973_debt-to-limi-ratio.html.

38. Donncha Marron, "'Lending by Numbers': Credit Scoring and the Constitution of Risk within American Consumer Credit," *Economics and Society* 36 (2007): 111. For another black box analogy, see Martha Poon, "From New Deal Institutions to Capital Markets: Commercial Consumer Risk Scores and the Making of Subprime Mortgage Finance," *Accounting, Organizations and Society* 34 (2009): 654–674.

39. Theodore M. Porter, *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life* (Princeton: Princeton University Press, 1996), 45 ("Numbers create and can be compared with norms, which are among the gentlest and yet most pervasive forms of power in modern democracies.").

40. See, e.g., Shawn Fremstad and Amy Traub, *Discrediting America: The Urgent Need to Reform the Nation's Credit Reporting Industry* (New York: Dēmos,

2011), 11. Available at http://www.demos.org/sites/default/files/publications/Discrediting_America_Demos.pdf.

41. Jeffrey Zaslow, "If TiVo Thinks You Are Gay, Here's How to Set It Straight," *Wall Street Journal*, November 26, 2002, http://online.wsj.com/news/articles/SB10382619368723569O8.

42. Matthew Moore, "Gay Men Can Be Identified by Their Facebook Friends," *The Telegraph*, September 21, 2009, http://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html.

43. Katie Heaney, "Facebook Knew I Was Gay before My Family Did," *BuzzFeed*, March 19, 2013, http://www.buzzfeed.com/katieheaney/facebook-knew-i-was-gay-before-my-family-did.

44. Ellen Jean Hirst, "Critics Take Aim at Data Mining after OfficeMax Addresses a Letter to Father with Line, 'Daughter Killed in Car Crash'," *Chicago Tribune*, January 21, 2014, 1.

45. Casey Johnston, "Data Brokers Won't Even Tell the Government How It Uses, Sells Your Data," *Ars Technica* (blog), December 21, 2013, http://arstechnica.com/business/2013/12/data-brokers-wont-even-tell-the-government-how-it-uses-sells-your-data/.

46. Pam Dixon and Robert Gellman, *The Scoring of America* (San Diego: World Privacy Forum, 2014).

47. Frank A. Pasquale and Tara Adams Ragone, "The Future of HIPAA in the Cloud," *Stanford Technology Law Review* (forthcoming 2014). Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2298158.

48. A company called Acxiom has 1,600 pieces of information about 98 percent of U.S. adults, gathered from thousands of sources. Eli Pariser, *The Filter Bubble* (New York: Penguin, 2011), 3. At least some of them are health-indicative or health-predictive. Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven, CT: Yale University Press, 2008); Natasha Singer, "You for Sale: Mapping the Consumer Genome," *New York Times*, June 16, 2012; Nicolas P. Terry, "Protecting Patient Privacy in the Age of Big Data," *UMKC Law Review* 81 (2012): 385–416.

49. Chad Terhune, "They Know What's in Your Medicine Cabinet," *BusinessWeek*, July 22, 2008.

50. Terhune, "They Know What's in Your Medicine Cabinet." While PPACA would make those gains harder for health insurers now, there are many other contexts where it is profitable to avoid doing business with a person marked as sick.

51. Intelliscript Complaint, In the Matter of Milliman, Inc. (2008) (No. C-4213), http://www.ftc.gov/os/caselist/0623189/080212complaint.pdf.

52. William W. Yu and Trena M. Ezzati-Rice, "Concentration of Health Care Expenses in the U.S. Civilian Noninstitutionalized Population," Agency for Healthcare Research and Quality Statistical Brief No. 81, 2005. Available at http://www.meps.ahrq.gov/mepsweb/data_files/publications/st81/stat81.shtml.

53. They would be "guaranteed issue" of insurance now, given the 2010 Patient Protection and Affordable Care Act (PPACA). 42 U.S.C § 1201(4), 42 U.S.C § 2702(a)–(b)(1), 42 U.S.C. § 300gg-1(a)–(b)(1) (requiring acceptance of

all applicants, but allowing limitation to certain "open or special enrollment" periods).

54. Terry, "Protecting Patient Privacy."

55. Ibid. (Those who "fill out warranty cards, enter sweepstakes, answer online surveys, agree to online privacy policies or sign up to receive e-mails from brands, they often don't realize that certain details—linked to them by name or by customer ID code—may be passed along to other companies.")

56. Lori Andrews, *I Know Who You Are and I Saw What You Did* (New York: Free Press, 2011), 70. Andrews uses the term "weblining" (an echo of the discriminatory lending practice, "redlining") to suggest how internet profiling can create new minorities who do not even know how they are being discriminated against.

57. Charles Duhigg, "How Companies Learn Your Secrets," *New York Times Magazine*, February 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

58. Elizabeth A. Harris and Nicole Perlroth, "For Target, the Breach Numbers Grow," *New York Times*, January 1, 2014, http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0.

59. Thomas R. McLean & Alexander B. McLean, "Dependence on Cyberscribes-Issues in E-Security," *8 J. Bus. & Tech. L.* (2013): 59 (discussing instances of medical information on the black market); Brian Krebs & Anita Kumar, "Hackers Want Millions for Data on Prescriptions," *Wash. Post*, May 8, 2009, at B1.

60. Misha Glenny, *DarkMarket: How Hackers Became the New Mafia* (New York: Vintage Books, 2012) 2 ("this minuscule elite (call them geeks, technos, hackers, coders, securocrats, or what you will) has a profound understanding of a technology that every day directs our lives more intensively and extensively, while most of the rest of us understand absolutely zip about it.").

61. "Experian Sold Consumer Data to ID Theft Service," *Krebs on Security*, October 20, 2013, http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/.

62. Duhigg, "How Companies Learn Your Secrets."

63. Ryan Calo, "Digital Market Manipulation," *George Washington University Law Review* (forthcoming, 2014), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703&download=yes.

64. PRNewsWire, "New Beauty Study Reveals Days, Times and Occasions When U.S. Women Feel Least Attractive," October 2, 2013 (news release), http://www.prnewswire.com/news-releases/new-beauty-study-reveals-days-times-and-occasions-when-us-women-feel-least-attractive-226131921.html.

65. Paul Ohm coined the term "database of ruin" to suggest how damaging information could accumulate about a person. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *University of California at Los Angeles Law Review* 57 (2010): 1750–51.

66. Joseph Walker, "Data Mining to Recruit Sick People," *Wall Street Journal*, December 17, 2013, http://online.wsj.com/news/articles/SB10001424052702303722104579240140554518458. The *Journal* tries to explain these Big

Data associations by hypothesizing that large men need minivans because they cannot fit into other vehicles. But note how easily we could also rationalize the opposite conclusion: if minivan drivers were pegged as exceptionally fit, we might hypothesize that they used the large vehicle to carry around sports equipment. We should beware post hoc rationalizations of Big Data correlations, particularly when we are unable to review the representativeness of the data processed or the algorithms used to process it.

67. Ibid.

68. Some privacy protective measures are taken with respect to search logs. But, as Nissenbaum and Toubiana observe, "Without an external audit of these search logs, it is currently impossible to evaluate their robustness against de-anonymizing attacks." V. Toubiana and H. Nissenbaum, "An Analysis of Google Log Retention Policies," *The Journal of Privacy and Confidentiality* 3, no. 1 (2011): 5. For a search query revelation that proved revealing, despite anonymization efforts, see Thomas Barbaro and Michael Zeller, "A Face Is Exposed for AOL Searcher No. 44417749," *New York Times*, August 9, 2006, A1.

69. Walker, "Data Mining to Recruit Sick People."

70. Julie Brill, "Reclaim Your Name," Keynote Address at Computers, Freedom, and Privacy Conference, June 26, 2013. Available at http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf.

71. Ibid. ("One health insurance company recently bought data on more than three million people's consumer purchases in order to flag health-related actions, like purchasing plus-sized clothing, the *Wall Street Journal* reported. [The company bought purchasing information for current plan members, not as part of screening people for potential coverage.]")

72. Peter Maass, "Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless," *Wired*, June 28, 2012, http://www.wired.com/threatlevel/2012/06/ftc-fail/all/.

73. Charles Duhigg, "What Does Your Credit Card Company Know about You?" *New York Times*, May 17, 2009, http://www.nytimes.com/2009/05/17/magazine/17credit-t.html?pagewanted=all. For a compelling account for the crucial role that the FTC plays in regulating unfair consumer practices and establishing a common law of privacy, see Daniel J. Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," *Columbia Law Review* 114 (2014): 583–676.

74. Duhigg, "What Does Your Credit Card Company Know about You?"

75. Kashmir Hill, "Could Target Sell Its 'Pregnancy Prediction Score'?" *Forbes*, February 16, 2012, http://www.forbes.com/sites/kashmirhill/2012/02/16/could-target-sell-its-pregnancy-prediction-score/.

76. Frank Pasquale, "Reputation Regulation: Disclosure and the Challenge of Clandestinely Commensurating Computing," in *The Offensive Internet: Speech, Privacy, and Reputation*, ed. Saul Levmore and Martha C. Nussbaum (Cambridge, MA: Harvard University Press, 2010), 107–123; Frank Pasquale, "Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries," *Northwestern University Law Review* 104 (2010): 105–174.

77. Lois Beckett, "Everything We Know about What Data Brokers Know about You," *ProPublica*, March 7, 2013 (updated September 13, 2013), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

78. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012). Available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (providing list of types of data brokers).

79. Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (New Haven, CT: Yale University Press, 2012).

80. Natasha Singer, "Secret E-Scores Chart Consumers' Buying Power," *New York Times*, August 18, 2012, http://www.nytimes.com/2012/08/19/business/electronic-scores-rank-consumers-by-potential-value.html?_r=0&pagewanted=print.

81. Dixon and Gellman, *The Scoring of America*.

82. Ylan Q. Mui, "Little-Known Firms Tracking Data Used in Credit Scores," *Washington Post*, July 16, 2011, http://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gIQAXHcWII_print.html. The firm was ChoicePoint (now a part of another, larger firm), a data broker that maintained files on nearly all Americans.

83. Many data brokers double as reputational intermediaries, offering rankings and scores that promise to simplify the data reports they can prepare about individuals. They admit their work is a black box, given the "veil of secrecy surrounding the origins of the information, how it is analyzed and who buys it." Mui, "Little-Known Firms."

84. Ibid., 79.

85. Sherry D. Sanders, "Privacy Is Dead: The Birth of Social Media Background Checks," *39 Southwestern University Law Review 243*, (2012): 264; Alexander Reicher, "The Background of Our Being: Internet Background Checks in the Hiring Process," *28 Berkeley Tech. L.J.* (2013): 153.

86. Don Peck, "They're Watching You at Work," *The Atlantic*, December 2013, 76. When work is largely done in computing environments, the assessment can be very granular. Software engineers are assessed for their contributions to open source projects, with points awarded when others use their code. E. Gabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton, NJ: Princeton University Press, 2013) (exploring Debian open source community and assessment of community members' contributions); Stephen Baker, *The Numerati* (New York: Houghton-Mifflin, 2008), 33.

87. Mat Honan, "I Flunked My Social Media Background Check. Will You?," *Gizmodo* (July 7, 2011). Available at http://gizmodo.com/5818774/this-is-a-social-media-background-check/. ("For each [social media] internet sources, Social Intelligence scored [candidate as] either "pass" or "negative," and included comments such as "subject admits to use of cocaine as well as LSD," and "subject references use of Ketamine [another recreational drug].").

88. Solove, *The Digital Person*, 47.

89. Tom Burghardt, "Big Brother a Click Away," *Pacific Free Press*, October 10, 2010, http://www.pacificfreepress.com/news/1/7119-big-brother-a-click-away.html. See also Mickey Huff and Project Censored, *Censored 2012: The Top Censored Stories and Media Analysis of 2010–2011* (New York: Seven Stories Press, 2011), 61. The venture capital companies Google Ventures and In-Q-Tel invested in Recorded Future.

90. Peck, "They're Watching You at Work."

91. Lewis Maltby, *Can They Do That? Retaking Our Fundamental Rights in the Workplace* (New York: Portfolio, 2009), 20 (describing pervasive surveillance); Chris Bertram, "Let It Bleed: Libertarians and the Workplace," *Crooked Timber* (blog), July 1, 2012, http://crookedtimber.org/2012/07/01/let-it-bleed-libertarianism-and-the-workplace/. ("On pain of being fired, workers in most parts of the United States can be commanded to pee or forbidden to pee. They can be watched on camera by their boss while they pee.")

92. Employee consent is an affirmative defense against employee causes of action based on invasion of privacy. Larry O. Natt Gantt, II, "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace," *8 Harv. J.L. & Tech.* (1995): 345, 375. Courts will at times not allow this defense if it goes against certain public policy interests or if a statute forbids such specific aspects of the waiver. See, e.g., Speer v. Ohio Dept. of Rehab. & Corr., 624 N.E.2d 251 (Ohio, 1993) (forbidding waiver of right to privacy in employer's bathroom).

93. William Bogard, *The Simulation of Surveillance: Hypercontrol in Telematic Societies* (Cambridge: Cambridge University Press, 1996).

94. Peck, "They're Watching You at Work."

95. Leigh Buchanan, "Unemployment Is Up. Why Is It So Hard to Find the Right Hires?" *Inc.*, June 1, 2012, http://www.inc.com/leigh-buchanan/hiring-recruiting-unemployment-wharton-peter-cappelli.html.

96. Peter Cappelli, *Why Good People Can't Get Jobs: The Skills Gap and What Companies Can Do about It* (Philadelphia, PA: Wharton Digital Press, 2012).

97. They "processed about 29 applications for every opening in 2008, up from 22 in 2007." Vanessa O'Connell, "Test for Dwindling Retail Jobs Spawns a Culture of Cheating," *Wall Street Journal*, January 7, 2009, http://online.wsj.com/article/SB123129220146959621.html?mod=googlenews_wsj; Christopher Ingraham, "Wal-Mart Has a Lower Acceptance Rate than Harvard," *Washington Post*, Mar. 28, 2014, at http://www.washingtonpost.com/blogs/wonkblog/wp/2014/03/28/wal-mart-has-a-lower-acceptance-rate-than-harvard/.

98. Barbara Ehrenreich, "Time Theft," *New Internationalist Magazine*, November 2, 2002, http://www.newint.org/features/2002/11/01/women/.

99. O'Connell, "Test for Dwindling Retail Jobs Spawns a Culture of Cheating."

100. Chris Anderson, "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete," *Wired*, June 23, 2008, http://www.wired.com/science/discoveries/magazine/16-07/pb_theory.

101. Ibid.

102. Charles Tilly, *Why?: What Happens When Persons Give Reasons* (Princeton: Princeton University Press, 2008).

103. Omer Tene and Jules Polonetsky, "A Theory of Creepy: Technology, Privacy and Shifting Social Norms," *Yale Journal of Law and Technology* 16 (2014): 59–102.

104. Leon R. Kass, "The Wisdom of Repugnance," *The New Republic*, June 1997; Martha C. Nussbaum, *Upheavals of Thought: The Intelligence of Emotions* (New York: Cambridge University Press, 2001).

105. Bruce Schneier, "Will Giving the Internet Eyes and Ears Mean the End of Privacy?" *The Guardian*, May 16, 2013, http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google.

106. Danielle Keats Citron, "Technological Due Process," *Washington University Law Review* 85 (2008): 1260–1263; Danielle Keats Citron, "Open Code Governance," *University of Chicago Legal Forum* (2008): 363–368.

107. Peck, "They're Watching You at Work."

108. Lior Jacob Strahilevitz, "Less Regulation, More Reputation," in *The Reputation Society: How Online Opinions Are Reshaping the Offline World*, ed. Hassan Masum and Mark Tovey (Cambridge, MA: MIT Press, 2012), 64.

109. Associated Press, "EEOC Sues over Criminal Background Checks," *CBSNews*, June 11, 2013, http://www.cbsnews.com/8301-505123_162-57588814/eeoc-sues-over-criminal-background-checks/.

110. Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (2014).

111. David Talbot, "Data Discrimination Means the Poor May Experience a Different Internet," *Technology Review*, Oct. 9, 2013, at http://www.technologyreview.com/news/520131/data-discrimination-means-the-poor-may-experience-a-different-internet/ (discussing work of Kate Crawford and Jason Schultz).

112. Devony B. Schmidt, "Researchers Present Findings on Online Criminal Record Websites," *The Harvard Crimson*, November 20, 2012, http://www.thecrimson.com/article/2012/11/20/research-finds-profiling/.

113. Latanya Sweeney, "Discrimination in Online Ad Delivery," *Communications of the ACM* 56 (2013): 44. She ultimately found "statistically significant discrimination in ad delivery based on searches of 2184 racially associated personal names," in that ads suggesting arrest (as in the question, Arrested?) were likely to appear in the context of names associated with blacks even when there was no actual arrest record. See generally Seeta Gangadaran, "Digital Inclusion and Data Profiling," *First Monday*, 5 (2012).

114. "Racism Is Poisoning Online Ad Delivery, Professor Says," *MIT Technology Review*, February 4, 2013, http://www.technologyreview.com/view/510646/racism-is-poisoning-online-ad-delivery-says-harvard-professor/.

115. Toon Calders & Indre Zliobaite, "Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures," in *Discrimination and Privacy in the Information Society* (Bart Custers, et al., eds.) (Heidelberg: Springer, 2013).

116. Max Nisen, "Only 2% of Google's American Workforce Is Black," *The Atlantic*, May 29, 2014, at http://www.theatlantic.com/business/archive/2014/05/only-2-percent-of-googles-american-workforce-is-black/371805/.

117. Nathan Newman, "Racial and Economic Profiling in Google Ads: A Preliminary Investigation (Updated)," *Huffington Post* (blog), September 20, 2011, http://www.huffingtonpost.com/nathan-newman/racial-and-economic-profi_b_970451.html. (Some of Newman's work has been funded by Microsoft, a Google rival.)

118. Ibid.

119. FTC, "Spring Privacy Series: Alternative Scoring Products," March 19, 2014 (news release), http://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.

120. FTC chair Edith Ramirez has voiced her concerns about algorithms that judge individuals "not because of what they've done, or what they will do in the future, but because inferences or correlations drawn by algorithms suggest they may behave in ways that make them poor credit or insurance risks, unsuitable candidates for employment or admission to schools or other institutions, or unlikely to carry out certain functions." Edith Ramirez, "Privacy Challenges in the Era of Big Data: The View from the Lifeguard's Chair," Keynote Address at the Technology Policy Institute Aspen Forum, August 19, 2013. Available at http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf.

121. Ibid.

122. Michael Pinard, "Collateral Consequences of Criminal Convictions: Confronting Issues of Race and Dignity," *New York University Law Review* 85 (2010): 457–534.

123. Key policymakers in the Obama administration issued a report on the issue, and stated "A key finding of this report is that big data could enable new forms of discrimination and predatory practices." Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (Washington, D.C., 2014), at 53.

124. Interview by Doug Henwood, Behind the News, with Sarah Ludwig, NEDAP Attorney, on *Behind the News Radio* (August 30, 2007). Available at http://www.leftbusinessobserver.com/Radio.html.

125. See generally Jerry Kang, *Implicit Bias: A Primer for Courts* (Williamsburg, VA: National Center for State Courts, 2009). Available at http://wp.jerrykang.net.s110363.gridserver.com/wp-content/uploads/2010/10/kang-Implicit-Bias-Primer-for-courts-09.pdf.

126. Cf. Loïc Wacquant, "The Punitive Regulation of Poverty in the Neoliberal Age," *OpenDemocracy*, August 1, 2011, http://www.opendemocracy.net/5050/lo%C3%AFc-wacquant/punitive-regulation-of-poverty-in-neoliberal-age. See generally Bernard E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (Chicago: University of Chicago Press, 2007).

127. Cf. Robert E. Goodin, "Laundering Preferences," in *Foundations of Social Choice Theory*, ed. Jon Elster and Aanund Hylland (Cambridge, UK: Cambridge University Press, 1989), 75.

128. Charles Taylor, *Philosophical Papers II: Philosophy and the Human Sciences* (New York: Cambridge University Press, 1986). Data-driven analytics promises a more scientific approach to credit allocation and marketing than narrative

histories or one-dimensional scoring. But "objective analysis" can morph into objectification, just as "more rational" credit scoring led to rationalizations of toxic subprime loans.

129. Marx W. Wartofsky, *Conceptual Foundations of Scientific Thought* (New York: Macmillan, 1968).

130. Alice Goffman, *On the Run: Fugitive Life in an American City* (Chicago: University of Chicago Press, 2014); Matt Taibbi, *The Divide* (New York: Spiegel & Grau, 2014).

131. As Charles Taylor puts it, "By 'brute data' I mean . . . data whose validity cannot be questioned by offering another interpretation or reading. . . ." Taylor, *Philosophical Papers*, *Vol. II*, 19.

132. Harcourt, *Against Prediction*, 156.

133. See, e.g., Floyd v. City of New York, Case No. 1:08-cv-01034-SAS-HBP (Aug. 12, 2013), 58. Available at http://ccrjustice.org/files/Floyd-Liability-Opinion-8-12-13.pdf. (The court found that "the NYPD [New York Police Department] has an unwritten policy of targeting racially defined groups for stops.")

134. William Harless, "'Ban the Box' Laws Make Criminal Pasts Off-Limits," *Wall Street Journal*, August 3, 2013, http://online.wsj.com/news/articles/SB10001424127887323997004578640623464096406.

135. Radley Balko, *Rise of the Warrior Cop: The Militarization of America's Police Forces* (New York: Public Affairs, 2013).

136. Daniel Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven, CT: Yale University Press, 2011).

137. Gregory B. Hladky, "Arrest Exposes State's Threats List," *New Haven Register*, January 9, 2007, A1. Christine Stuart, "Reporter Arrested for Political Activism," *Connecticut News Junkie* (blog), January 5, 2007, http://www.ctnewsjunkie.com/ctnj.php/archives/entry/reporter_arrested_for_political_activism_updated_with_police_report/. Gerri Willis, "Are You on the List?," *CNN*, September 30, 2009, http://www.cnn.com/video#/video/crime/2009/09/30/willis.fusion.centers.cnn.

138. *Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing: Hearing before the Subcomm. on Terrorism, Technology, and Homeland Security of the S. Comm. on the Judiciary*, 111th Cong. 56–57 (2009) (statement of Caroline Fredrickson, Director, Washington Office, ACLU); Lisa Rein, "Police Spied on Activists in Maryland," *Washington Post*, July 18, 2008, A1; Office of Senator Barbara Mikulski, "Senators Demand Answers," February 19, 2009 (news release), http://mikulski.senate.gov/media/pressrelease/02-19-2009-2.cfm.

139. Matthew Harwood, "Maryland State Police Spied on Nonviolent Activists and Labeled Them Terrorists," *Security Management*, October 8, 2008, http://www.securitymanagement.com/news/maryland-state-police-spied-nonviolent-activists-and-labeled-them-terrorists-004742; Rein, "Police Spied on Activists in Maryland."

140. ACLU, "Policing Free Speech" (June 2010). Available at https://www.aclu.org/files/assets/Spyfiles_2_0.pdf.

141. See, e.g., Jennifer Stisa Granick and Christopher Jon Sprigman, Op-Ed, "The Criminal N.S.A.," *New York Times*, June 28, 2013, http://www.nytimes

.com/2013/06/28/opinion/the-criminal-nsa.html?ref=opinion&_r=2&; Jennifer Stisa Granick and Christopher Jon Sprigman, "NSA, DEA, IRS Lie about Fact That Americans Are Routinely Spied on by Our Government: Time for a Special Prosecutor," *Forbes*, August 14, 2013, http://www.forbes.com/sites/jennifergranick/2013/08/14/nsa-dea-irs-lie-about-fact-that-americans-are-routinely-spied-on-by-our-government-time-for-a-special-prosecutor-2/.

142. Pam Martens, "Wall Street Firms Spy on Protestors in Tax-Funded Center," *CounterPunch*, October 18, 2011, http://www.counterpunch.org/2011/10/18/wall-street-firms-spy-on-protestors-in-tax-funded-center/.

143. Ibid.

144. Colin Moynihan, "Officials Cast Wide Net in Monitoring Occupy Protests," *New York Times*, May 22, 2014, at http://www.nytimes.com/2014/05/23/us/officials-cast-wide-net-in-monitoring-occupy-protests.html.

145. Naomi Wolf, "The Shocking Truth about the Crackdown on Occupy," *The Guardian*, November 25, 2011, http://www.theguardian.com/commentisfree/cifamerica/2011/nov/25/shocking-truth-about-crackdown-occupy. Naomi Wolf, "Revealed: How the FBI Coordinated the Crackdown on Occupy," *The Guardian*, December 29, 2012, http://www.theguardian.com/commentisfree/2012/dec/29/fbi-coordinated-crackdown-occupy.

146. Partnership for Civil Justice Fund, "FBI Documents Reveal Secret Nationwide Occupy Monitoring," December 22, 2012. Available at http://www.justiceonline.org/commentary/fbi-files-ows.html.

147. Matthew Stoller, "Occupy Wall Street Is a Church of Dissent," *Naked Capitalism* (blog), September 29, 2011, http://www.nakedcapitalism.com/2011/09/matt-stoller-occupywallstreet-is-a-church-of-dissent-not-a-protest.html. W.J.T. Mitchell, Bernard E. Harcourt, and Michael Taussig, *Occupy: Three Inquiries in Disobedience* (Chicago: University of Chicago Press, 2013).

148. See essays in Susan Will, Stephen Handelman, and David C. Brotherton, eds., *How They Got Away with It: White Collar Criminals and the Financial Meltdown* (New York: Columbia University Press, 2013).

149. "FBI Documents Reveal Secret," *Partnership for Civil Justice Fund*, December 22, 2012, http://www.justiceonline.org/commentary/fbi-files-ows.html. Yves Smith, "Banks Deeply Involved in FBI-Coordinated Suppression of 'Terrorist' Occupy Wall Street," *Naked Capitalism* (blog), December 30, 2010, http://www.nakedcapitalism.com/2012/12/banks-deeply-involved-in-fbi-coordinated-suppression-of-terrorist-occupy-wall-street.html. Wolf, "Revealed."

150. Martens, "Wall Street Firms Spy on Protestors in Tax-Funded Center."

151. Department of Homeland Security, "Secretary Napolitano Unveils 'Virtual USA' Information-Sharing Initiative," December 9, 2009 (news release), http://www.dhs.gov/news/2009/12/09/virtual-usa-information-sharing-initiative.

152. Department of Homeland Security, "National Network of Fusion Centers Fact Sheet." Available at http://www.dhs.gov/national-network-fusion-centers-fact-sheet (accessed February 17, 2014).

153. Mike German and Jay Stanley, "Fusion Center Update," *ACLU* (July 2008), 12. Available at https://www.aclu.org/files/pdfs/privacy/fusion_update

_20080729.pdf; see Mark A. Randol, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, CRS Report for Congress, RL 40602 (2010), 11 (noting that there are seventy-two fusion centers).

154. Moynihan, "Officials Cast Wide Net."

155. *Beyond ISE Implementation: Exploring the Way Forward for Information Sharing: Hearing before Intelligence, Information Sharing, and Terrorism Risk Assessment Subcomm. on Homeland Security*, 111th Cong. 18 (2009). Robert O'Harrow, Jr., "Centers Tap into Personal Databases," *Washington Post*, April 2, 2008, A1. (As fusion center officials note, "There is never ever enough information. . . . That's what post-9/11 is about.")

156. Ryan Singel, "Fusion Centers Analyzing Reams of Americans' Personal Information," *Wired*, April 2, 2008, http://www.wired.com/threatlevel/2008/04/fusion-centers/.

157. Michael German and Jay Stanley, "What's Wrong with Fusion Centers?" ACLU (December 2007), 12; see Randol, *The Department of Homeland Security Intelligence Enterprise*, 11.

158. Michael Fickes, "The Power of Fusion," *American City & County*, March 1, 2008, http://americancityandcounty.com/security/homeland/power_fusion_nsa. Matthew Harwood, "Port of Long Beach Fusion Center Opens," *Security Management*, February 9, 2009, http://www.securitymanagement.com/news/port-long-beach-fusion-center-opens-005197/.

159. Tom Monahan, "Safeguarding America's Playground," *UNLV Institute for Security Studies*, July/August 2010.

160. Some of them even attest to that inclusiveness in their names. Department of Homeland Security, "Fusion Center Locations," https://www.dhs.gov/fusion-center-locations-and-contact-information (accessed May 22, 2014). G.W. Schulz, "Homeland Security USA: Obama Wants to Hire 'Thousands' for Domestic Intel," *The Center for Investigative Reporting* (blog), March 10, 2009, http://cironline.org/blog/post/homeland-security-usa-obama-wants-hire-%E2%80%98thousands%E2%80%99-domestic-intel-486

161. Torin Monahan, *Surveillance in the Time of Insecurity* (Piscataway, NJ: Rutgers University Press, 2010), 46.

162. Ibid.

163. John Rollins, *Fusion Centers: Issues and Options for Congress*, CRS Report for Congress, RL34070 (January 2008), 21.

164. According to the CRS report, "less than 15% of fusion centers interviewed for [the report] described their mission as solely counterterrorism. In the last year, many counterterrorism-focused centers have expanded their mission to include all-crimes and/or all-hazards." Rollins, *Fusion Centers: Issues and Options*, 21.

165. Christopher Slobogin, "Surveillance and the Constitution," *Wayne Law Review* 55 (2009): 1118.

166. John Shiffman and Kristina Cooke, "Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans," Reuters, August 5, 2013, http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

167. Quoted in Michael Coleman, "Ex-CIA, NSA Chief Defends U.S. Intelligence Gathering," *The Washington Diplomat*, August 28, 2013, http://www.washdiplomat.com/index.php?option=com_content&view=article&id=9543&Itemid=414.

168. United States Senators Tammy Baldwin, Ron Wyden, Sherrod Brown, Tom Udall, and Richard Blumenthal, Letter to the Honorable Eric Holder, August 22, 2013. Available at https://www.fas.org/irp/congress/2013_cr/nsa-dea.pdf.

169. U.S. Department of Homeland Security, *Civil Liberties Impact Assessment for the State, Local, and Regional Fusion Center Initiative* (2008), 2.

170. Rollins, *Fusion Centers: Issues and Options*, 41–42.

171. Schulz, "Homeland Security USA."

172. Examples in Danielle Keats Citron and Frank Pasquale, "Network Accountability for the Domestic Intelligence Apparatus," *Hastings Law Journal* 62 (2011): 1441–1494; Pam Martens, "Wall Street's Secret Spy Center, Run for the 1% by NYPD," *CounterPunch*, February 6, 2012, http://www.counterpunch.org/2012/02/06/wall-streets-secret-spy-center-run-for-the-1-by-nypd/.

173. Spokesperson, California Anti-Terrorism Information Center, quoted in David E. Kaplan, "Spies among Us," *U.S. News and World Report*, May 8, 2006, 40.

174. Robert Mueller, FBI Director, quoted in Stephan Salisbury, "Surveillance, America's Pastime," *The Nation*, October 4, 2010, http://www.thenation.com/article/155158/surveillance-americas-pastime.

175. "2009 Virginia Terrorism Threat Assessment" (Mar. 2009). *Virginia Fusion Center*. Available at http://rawstory.com/images/other/vafusioncenterterrorassessment.pdf. Matthew Harwood, "Fusion Centers under Fire in Texas and New Mexico," *Security Management*, March 9, 2009.

176. "MIAC Strategic Report: The Modern Militia Movement," *Missouri Information Analysis Center*, February 20, 2009, http://constitution.org/abus/le/miac-strategic-report.pdf; see Chad Livengood, "Agency Apologizes for Militia Report on Candidates," *Springfield News-Leader*, March 10, 2009.

177. T.J. Greaney, "'Fusion Center' Data Draws Fire over Assertions," *Columbia Daily Tribune*, March 14, 2009, A1.

178. Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," *University of North Carolina Journal of International Law and Commercial Regulation* 29 (2004): 595–638.

179. Jon D. Michaels, "All the President's Spies: Private–Public Intelligence Partnerships in the War on Terror," 96 (2008): 915.

180. Solove, *The Digital Person*, 171.

181. Richard Hovel, Senior Adviser on Aviation and Homeland Security, Boeing Company, quoted in Alice Lipowicz, "Boeing to Staff FBI Fusion Center," *Washington Technology*, June 1, 2007, http://washingtontechnology.com/articles/2007/06/01/boeing-to-staff-fbi-fusion-center.aspx. ASIS International, "ASIS Foundation and Illinois Law Enforcement Create the First Private-Sector Funded Position for the Illinois Statewide Terrorism and Intelligence Fusion Center," April 21, 2009 (news release), https://www.asisonline

.org/News/Press-Room/Press-Releases/2009/Pages/FirstPrivateSectorFunded-Position.aspx. Lipowicz, "Boeing to Staff FBI Fusion Center"; "Novel Fusion Center to Boost Anti-Fraud Efforts in California," *Fraud Focus*, Summer 2008, 1. Available at http://www.insurancefraud.org/downloads/FF-Summer2008.pdf.

182. Joseph Straw, "Smashing Intelligence Stovepipes," *Security Management*, http://www.securitymanagement.com/article/smashing-intelligence-stovepipes (accessed May 22, 2014).

183. Michaels, "All the President's Spies," 914–916.

184. EPIC v. NSA, 798 F. Supp. 2d 26 (D.D.C. July 8, 2011).

185. Eric Limer, "How Google Gives Your Information to the NSA," Gizmodo, June 12, 2013, at http://gizmodo.com/how-google-gives-your-information-to-the-nsa-512840958.

186. James Glanz and Andrew Lehren, "N.S.A. Spied on Allies, Aid Groups and Businesses," *New York Times*, December 20, 2013, A1.

187. Gillian E. Metzger, "Privatization as Delegation," *Columbia Law Review* 103 (2003): 1378.

188. "An impressive number of top-ranking DHS officials have already [as of 2006] abandoned public service to serve the public by working and lobbying for . . . entrepreneurial firms, moves that often are associated with a considerable increase in salary—from $155,000 per year to $934,000 in one case." John Mueller, *Overblown* (New York: Free Press, 2009), 43, citing Eric Lipton, "Former Antiterror Officials Find That Industry Pays Better," *New York Times*, June 18, 2006, A1; Eric Lipton, "Company Ties Not Always Noted in Push to Tighten U.S. Security," *New York Times*, June 19, 2006, A1. See also Paul R. Verkuil, *Outsourcing Sovereignty: Why Privatization of Government Functions Threatens Democracy and What We Can Do about It* (New York: Cambridge University Press, 2007).

189. Consider Science Applications International Corporation (SAIC). Donald L. Bartlett and James B. Steele said in their reporting on SAIC, "No Washington contractor pursues government money with more ingenuity and perseverance than SAIC . . . [and] no contractor cloaks its operations in greater secrecy." Donald L. Barlett and James B. Steele, "Washington's $8 Billion Shadow," *Vanity Fair*, March 2007 http://www.vanityfair.com/politics/features/2007/03/spyagency200703. Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing* (New York: Simon & Schuster, 2008).

190. Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (London: Vintage, 2014).

191. Government entities mine data from social media sites for the purpose of trying to identify potential school shooters and terrorists. This type of practice, of course, comes with a high risk of false positives. Gabe Rottman, "Open Source Intelligence and Crime Prevention," *ACLU: Free Future* (blog), December 21, 2012, https://www.aclu.org/blog/technology-and-liberty-national-security-free-speech/open-source-intelligence-and-crime.

192. Hoofnagle, "Big Brother's Little Helpers."

193. Even its institutions of oversight are secretive, leaving journalists to rely on spectacular leaks like that of Edward Snowden (or well-cultivated sources, like James Bamford's at the NSA).

194. Stephen Benavides, "Outsourced Intelligence: How the FBI and CIA Use Private Contractors to Monitor Social Media," *Truthout*, June 13, 2013, http://truth-out.org/news/item/16943-outsourced-intelligence-how-the-fbi-and-cia-use-private-contractors-to-monitor-social-media.

195. Though perhaps not greater than the sum of terror threats—a question presently explored via cost-benefit analysis, but probably better addressed in scenario planning.

196. Foucault charted the classic contrast between spectacular exercises of power, and insidious biopower. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Trans. Alan Sheridan) (New York: Vintage Books, 1979). For more on the relative importance of fast and slow violence, see Rob Nixon, *Slow Violence and the Environmentalism of the Poor* (Cambridge: Harvard University Press, 2011).

197. Jathan Sadowski, "Why We Should Wash Our Hands of 'Cyber-Hygiene,'" *Slate* (blog), June 13, 2013, http://www.slate.com/blogs/future_tense/2013/06/19/cyber_hygiene_vint_cerf_s_concept_of_personal_cybersecurity_is_problematic.html.

198. Finn Brunton and Helen Nissenbaum, "Political and Ethical Perspectives on Data Obfuscation," in *Privacy, Due Process and the Computational Turn*, ed. Mireille Hildebrandt and Katja de Vries (New York: Routledge, 2013), 171; Finn Brunton and Helen Nissenbaum, "Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation," *First Monday* 16, no. 5 (May 2011), http://firstmonday.org/article/view/3493/2955.

199. Adam Ostrow, "Track Who's Tracking You with Mozilla Collusion," *Mashable*, February 28, 2012, http://mashable.com/2012/02/28/mozilla-collusion/.

200. Jerry Kang, Katie Shilton, Deborah Estrin and Jeff Burke, "Self-Surveillance Privacy," *Iowa Law Review* 97 (2010): 809–848; Jonathan Zittrain, "What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication," *Stanford Law Review* 52 (2000): 1201–1250; Latanya Sweeney, *The Data Map* (2012), http://thedatamap.org/maps.html.

201. Though some regulators are setting security standards, the leading policy response is simply to notify people that the breach occurred. Gina Stevens, *Federal Information Security and Data Breach Notification Laws*, CRS Report for Congress, RL34120 (2010).

202. Kim Zetter, "Use These Secret NSA Google Search Tips to Become Your Own Spy Agency," *Wired*, May 8, 2013, http://www.wired.com/threatlevel/2013/05/nsa-manual-on-hacking-internet/.

203. Lucas Mearian, "'Wall of Shame' Exposes 21M Medical Record Breaches," *Computerworld*, August 7, 2012, http://www.computerworld.com/s/article/9230028. Office of Civil Rights, Department of Health and Human Services, "Breaches Affecting 500 or More Individuals," http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (accessed May 21, 2014).

204. Jonathan Dame, "Will Employers Still Ask for Facebook Passwords in 2014?," *USA Today College*, January 10, 2014, http://www.usatoday.com/story/money/business/2014/01/05/facebook-passwords-employers/4327739/.

205. In Europe, there is a "right to be forgotten" that obliges data controllers like Google to respond if a data subject, "in the light of his fundamental rights under Articles 7 and 8 of the Charter, request[s] that the information in question no longer be made available to the general public on account of its inclusion in such a list of results," and his "rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name," unless "the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question." Google Inc. v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, May 13, 2014.

206. Timothy Lee, "Five Ways to Stop the NSA from Spying on You," *Washington Post Wonkblog*, June 10, 2013, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/10/five-ways-to-stop-the-nsa-from-spying-on-you/ (recommending Tor). Bruce Schneier, "Has Tor Been Compromised?," *Schneier on Security* (blog), August 6, 2013, https://www.schneier.com/blog/archives/2013/08/has_tor_been_co.html.

207. Julia Angwin, *Dragnet Nation* (New York: Times Books, 2014).

208. Sarah N. O'Donohue, "'Like' it or Not, Password Protection Laws Could Protect Much More than Passwords," *Journal of Law, Business, and Ethics* 20 (2014): 77, 80.

209. Peppet, "Unraveling Privacy."

210. Scott Peppet's article "Unraveling Privacy"[0] has described how individual behavior can render past models of privacy protection obsolete. Scott R. Peppet, "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future," *Northwestern Law Review* 105 (2011): 1153–1204.

211. Nicholas Shaxson, *Treasure Islands: Tax Havens and the Men Who Stole the World* (New York, NY: Vintage Books, 2012); Hedda Leikvang, "Piercing the Veil of Secrecy: Securing Effective Exchange of Information to Remedy the Harmful Effects of Tax Havens," *Vanderbilt Journal of Transnational Law* 45 (2012): 330; David Leigh, Harold Frayman, and James Ball, "Front Men Disguise the Offshore Game's Real Players" (Nov. 2012). *International Consortium of Investigative Journalists*. Available at http://www.icij.org/front-men-disguise-offshore-players.

212. James S. Henry, *The Price of Offshore Revisited* (Chesham, Buckinghamshire, UK: Tax Justice Network, 2012). Available at http://www.taxjustice.net/cms/upload/pdf/Price_of_Offshore_Revisited_120722.pdf.

213. International Consortium of Investigative Journalists and Center for Public Integrity, *Secrecy for Sale: Inside the Offshore Money Maze* (Washington, DC: Center for Public Integrity, 2013). Available at http://cloudfront-files-1.publicintegrity.org/documents/pdfs/ICIJ%20Secrecy%20for%20Sale.pdf. The report was only possible because of a "Wikileaks"-style breach exposing the contours of labyrinthine corporate structures designed to hide income sources. We can be sure the "wealth defense industry" is redoubling its investments in avoiding future leaks. Dan Froomkin, "'Wealth Defense Industry'

Protects 1% from the Rabble and Its Taxes," *Huffington Post* (blog), December 13, 2011, http://www.huffingtonpost.com/dan-froomkin/wealth-defense-industry-p_b_1145825.html.

214. Omri Marian, "Are Cryptocurrencies Super Tax Havens?," *Michigan Law Review First Impressions* 112 (2013): 38–48. Available at http://www.michiganlawreview.org/articles/are-cryptocurrencies-em-super-em-tax-havens.

215. Frank Pasquale, "Grand Bargains for Big Data: The Emerging Law of Health Information," *Maryland Law Review* 72 (2013): 682–772.

216. On the new economy as a system of social control and modulation, see Julie Cohen, *Configuring the Networked Self* (New Haven, CT: Yale University Press, 2012).

217. Letter of Thomas Jefferson to Isaac McPherson, August 13, 1813. Available at http://press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html.

3

The Hidden Logics of Search

1. David Stark, *The Sense of Dissonance: Accounts of Worth in Economic Life* (Princeton, NJ: Princeton University Press, 2009), 1.

2. On the use and abuse of the distinction between "IRL" (in real life) and virtual spaces, see Nicholas Carr, "Digital Dualism Denialism," *Rough Type* (blog), February 20, 2013, http://www.roughtype.com/?p=2090.

3. Rotten Tomatoes, http://www.rottentomatoes.com/; "Customer Reviews," *Amazon Help*. Available at http://www.amazon.com/gp/help/customer/display.html/?nodeId=12177361. Sam Costello, "Buying Music from the iTunes Store," *About.com*. Available at http://ipod.about.com/od/buyingfromitunesstore/ss/buying_itunes_3.htm.

4. Philip Evans and Thomas S. Wurster, *Blown to Bits: How the New Economics of Information Transforms Strategy* (Cambridge, MA: Harvard Business Review Press, 1999); Don Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence* (New York: McGraw-Hill, 1996).

5. Economist Richard Caves once observed that "buffs, buzz, and educated tastes" tended to serve as guides to culture. Richard Caves, *Creative Industries: Contracts between Art and Commerce* (Cambridge, MA: Harvard University Press, 2000), 175. Firms like Amazon, Apple, Google, and Facebook now serve as curators of the curators, making some "buzz" of some "buffs" prominent, and hiding others.

6. Phil Simon, *The Age of the Platform: How Amazon, Apple, Facebook, and Google Have Redefined Business* (Henderson, NV: Motion Publishing, 2011). Though we commonly only refer to Google as a "search engine," it's important to note that search functionality drives our experience of all these other Internet behemoths. Whereas *reputation* is the way the world "knows" us, our *searches* are increasingly the way we "know" the world. The scare quotes connote the slippages, obfuscations, and biases that modern finance imposes on these epistemic systems.