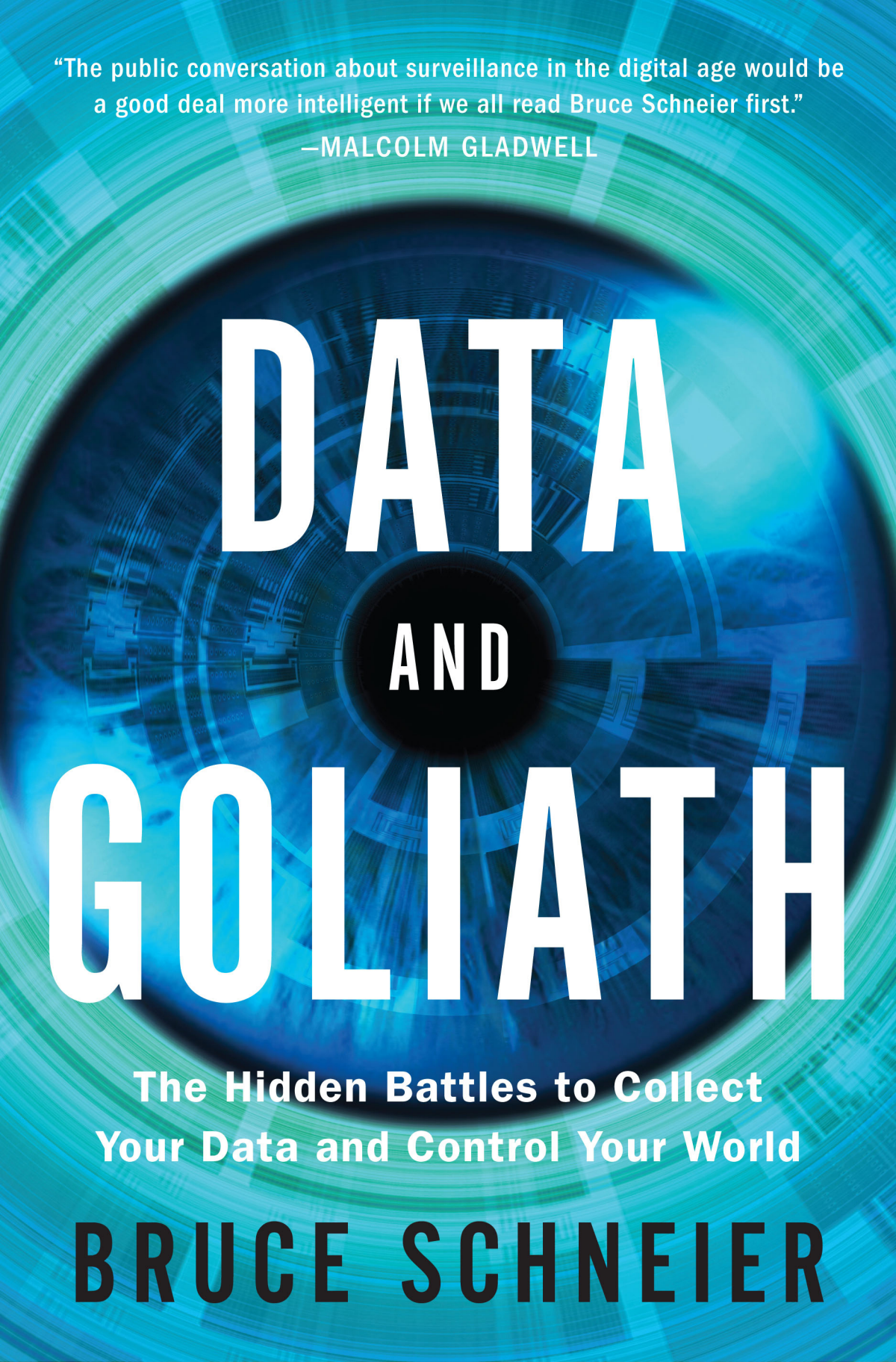
"The public conversation about surveillance in the digital age would be a good deal more intelligent if we all read Bruce Schneier first."
—MALCOLM GLADWELL



DATA AND GOLIATH

The Hidden Battles to Collect Your Data and Control Your World

BRUCE SCHNEIER

Introduction

If you need to be convinced that you're living in a science-fiction world, look at your cell phone. This cute, sleek, incredibly powerful tool has become so central to our lives that we take it for granted. It seems perfectly normal to pull this device out of your pocket, no matter where you are on the planet, and use it to talk to someone else, no matter where the person is on the planet.

Yet every morning when you put your cell phone in your pocket, you're making an implicit bargain with the carrier: "I want to make and receive mobile calls; in exchange, I allow this company to know where I am at all times." The bargain isn't specified in any contract, but it's inherent in how the service works. You probably hadn't thought about it, but now that I've pointed it out, you might well think it's a pretty good bargain. Cell phones really are great, and they can't work unless the cell phone companies know where you are, which means they keep you under their surveillance.

This is a very intimate form of surveillance. Your cell phone tracks where you live and where you work. It tracks where you like to spend your weekends and evenings. It tracks how often you go to church (and which church), how much time you spend in a bar, and whether you speed when you drive. It tracks—since it knows about all the other phones in your area—whom you spend your days with, whom you meet for lunch, and

whom you sleep with. The accumulated data can probably paint a better picture of how you spend your time than you can, because it doesn't have to rely on human memory. In 2012, researchers were able to use this data to predict where people would be *24 hours later*, to within 20 meters.

Before cell phones, if someone wanted to know all of this, he would have had to hire a private investigator to follow you around taking notes. Now that job is obsolete; the cell phone in your pocket does all of this automatically. It might be that no one retrieves that information, but it is there for the taking.

Your location information is valuable, and everyone wants access to it. The police want it. Cell phone location analysis is useful in criminal investigations in several different ways. The police can "ping" a particular phone to determine where it is, use historical data to determine where it has been, and collect all the cell phone location data from a specific area to figure out who was there and when. More and more, police are using this data for exactly these purposes.

Governments also use this same data for intimidation and social control. In 2014, the government of Ukraine sent this positively Orwellian text message to people in Kiev whose phones were at a certain place during a certain time period: "Dear subscriber, you have been registered as a participant in a mass disturbance." Don't think this behavior is limited to totalitarian countries; in 2010, Michigan police sought information about every cell phone in service near an expected labor protest. They didn't bother getting a warrant first.

There's a whole industry devoted to tracking you in real time. Companies use your phone to track you in stores to learn how you shop, track you on the road to determine how close you might be to a particular store, and deliver advertising to your phone based on where you are right now.

Your location data is so valuable that cell phone companies are now selling it to data brokers, who in turn resell it to anyone willing to pay for it. Companies like Sense Networks specialize in using this data to build personal profiles of each of us.

Phone companies are not the only source of cell phone data. The US company Verint sells cell phone tracking systems to both corporations and governments worldwide. The company's website says that it's "a global leader in Actionable Intelligence solutions for customer engage-

ment optimization, security intelligence, and fraud, risk and compliance," with clients in "more than 10,000 organizations in over 180 countries." The UK company Cobham sells a system that allows someone to send a "blind" call to a phone—one that doesn't ring, and isn't detectable. The blind call forces the phone to transmit on a certain frequency, allowing the sender to track that phone to within one meter. The company boasts government customers in Algeria, Brunei, Ghana, Pakistan, Saudi Arabia, Singapore, and the United States. Defentek, a company mysteriously registered in Panama, sells a system that can "locate and track any phone number in the world . . . undetected and unknown by the network, carrier, or the target." It's not an idle boast; telecommunications researcher Tobias Engel demonstrated the same thing at a hacker conference in 2008. Criminals do the same today.

All this location tracking is based on the cellular system. There's another entirely different and more accurate location system built into your smartphone: GPS. This is what provides location data to the various apps running on your phone. Some apps use location data to deliver service: Google Maps, Uber, Yelp. Others, like Angry Birds, just want to be able to collect and sell it.

You can do this, too. HelloSpy is an app that you can surreptitiously install on someone else's smartphone to track her. Perfect for an anxious mom wanting to spy on her teenager—or an abusive man wanting to spy on his wife or girlfriend. Employers have used apps like this to spy on their employees.

The US National Security Agency (NSA) and its UK counterpart, Government Communications Headquarters (GCHQ), use location data to track people. The NSA collects cell phone location data from a variety of sources: the cell towers that phones connect to, the location of Wi-Fi networks that phones log on to, and GPS location data from Internet apps. Two of the NSA's internal databases, code-named HAPPYFOOT and FASCIA, contain comprehensive location information of devices worldwide. The NSA uses the databases to track people's movements, identify people who associate with people of interest, and target drone strikes.

The NSA can allegedly track cell phones even when they are turned off.

I've just been talking about location information from one source—your cell phone—but the issue is far larger than this. The computers you

interact with are constantly producing intimate personal data about you. It includes what you read, watch, and listen to. It includes whom you talk to and what you say. Ultimately, it covers what you're thinking about, at least to the extent that your thoughts lead you to the Internet and search engines. We are living in the golden age of surveillance.

Sun Microsystems' CEO Scott McNealy said it plainly way back in 1999: "You have zero privacy anyway. Get over it." He's wrong about how we should react to surveillance, of course, but he's right that it's becoming harder and harder to avoid surveillance and maintain privacy.

Surveillance is a politically and emotionally loaded term, but I use it deliberately. The US military defines surveillance as "systematic observation." As I'll explain, modern-day electronic surveillance is exactly that. We're all open books to both governments and corporations; their ability to peer into our collective personal lives is greater than it has ever been before.

The bargain you make, again and again, with various companies is surveillance in exchange for free service. Google's chairman Eric Schmidt and its director of ideas Jared Cohen laid it out in their 2013 book, *The New Digital Age*. Here I'm paraphrasing their message: if you let us have all your data, we will show you advertisements you want to see and we'll throw in free web search, e-mail, and all sorts of other services. It's convenience, basically. We are social animals, and there's nothing more powerful or rewarding than communicating with other people. Digital means have become the easiest and quickest way to communicate. And why do we allow governments access? Because we fear the terrorists, fear the strangers abducting our children, fear the drug dealers, fear whatever bad guy is in vogue at the moment. That's the NSA's justification for its mass-surveillance programs; if you let us have all of your data, we'll relieve your fear.

The problem is that these aren't good or fair bargains, at least as they're structured today. We've been accepting them too easily, and without really understanding the terms.

Here is what's true. Today's technology gives governments and corporations robust capabilities for mass surveillance. Mass surveillance is dangerous. It enables discrimination based on almost any criteria: race, religion, class, political beliefs. It is being used to control what we see, what we can do, and, ultimately, what we say. It is being done without

offering citizens recourse or any real ability to opt out, and without any meaningful checks and balances. It makes us less safe. It makes us less free. The rules we had established to protect us from these dangers under earlier technological regimes are now woefully insufficient; they are not working. We need to fix that, and we need to do it very soon.

In this book, I make that case in three parts.

Part One describes the surveillance society we're living in. Chapter 1 looks at the varieties of personal data we generate as we go about our lives. It's not just the cell phone location data I've described. It's also data about our phone calls, e-mails, and text messages, plus all the webpages we read, our financial transaction data, and much more. Most of us don't realize the degree to which computers are integrated into everything we do, or that computer storage has become cheap enough to make it feasible to indefinitely save all the data we churn out. Most of us also underestimate just how easy it has become to identify us using data that we consider anonymous.

Chapter 2 shows how all this data is used for surveillance. It happens everywhere. It happens automatically, without human intervention. And it's largely hidden from view. This is ubiquitous mass surveillance.

It's easy to focus on how data is collected by corporations and governments, but that gives a distorted picture. The real story is how the different streams of data are processed, correlated, and analyzed. And it's not just one person's data; it's everyone's data. Ubiquitous mass surveillance is fundamentally different from just a lot of individual surveillance, and it's happening on a scale we've never seen before. I talk about this in Chapter 3.

Surveillance data is largely collected by the corporations that we interact with, either as customers or as users. Chapter 4 talks about business models of surveillance, primarily personalized advertising. An entire data broker industry has sprung up around profiting from our data, and our personal information is being bought and sold without our knowledge and consent. This is being driven by a new model of computing, where our data is stored in the cloud and accessed by devices like the iPhone that are under strict manufacturer control. The result is unprecedented corporate access to and control over our most intimate information.

Chapter 5 turns to government surveillance. Governments around the world are surveilling their citizens, and breaking into computers both

domestically and internationally. They want to spy on everyone to find terrorists and criminals, and—depending on the government—political activists, dissidents, environmental activists, consumer advocates, and freethinkers. I focus mainly on the NSA, because this is the secret government agency we know best, because of the documents Edward Snowden released.

Corporations and governments alike have an insatiable appetite for our data, and I discuss how the two work together in Chapter 6. I call it a "public-private surveillance partnership," and it's an alliance that runs deep. It's the primary reason that surveillance is so pervasive, and it will impede attempts to reform the system.

All of this matters, even if you trust the corporations you interact with and the government you're living under. With that in mind, Part Two turns to the many interrelated harms that arise from ubiquitous mass surveillance.

In Chapter 7, I discuss the harms caused by government surveillance. History has repeatedly demonstrated the dangers of allowing governments to conduct unchecked mass surveillance on their citizens. Potential harms include discrimination and control, chilling effects on free speech and free thought, inevitable abuse, and loss of democracy and liberty. The Internet has the potential to be an enormous driver of freedom and liberty around the world; we're squandering that potential by allowing governments to conduct worldwide surveillance.

Chapter 8 turns to the harms caused by unfettered corporate surveillance. Private companies now control the "places" on the Internet where we gather, and they're mining the information we leave there for their own benefit. By allowing companies to know everything about us, we're permitting them to categorize and manipulate us. This manipulation is largely hidden and unregulated, and will become more effective as technology improves.

Ubiquitous surveillance leads to other harms as well. Chapter 9 discusses the economic harms, primarily to US businesses, that arise when the citizens of different countries try to defend themselves against surveillance by the NSA and its allies. The Internet is a global platform, and attempts by countries like Germany and Brazil to build national walls

around their data will cost companies that permit government surveillance—particularly American companies—considerably.

In Chapter 10, I discuss the harms caused by a loss of privacy. Defenders of surveillance—from the Stasi of the German Democratic Republic to the Chilean dictator Augusto Pinochet to Google's Eric Schmidt—have always relied on the old saw "If you have nothing to hide, then you have nothing to fear." This is a dangerously narrow conception of the value of privacy. Privacy is an essential human need, and central to our ability to control how we relate to the world. Being stripped of privacy is fundamentally dehumanizing, and it makes no difference whether the surveillance is conducted by an undercover policeman following us around or by a computer algorithm tracking our every move.

In Chapter 11, I turn to the harms to security caused by surveillance. Government mass surveillance is often portrayed as a security benefit, something that protects us from terrorism. Yet there's no actual proof of any real successes against terrorism as a result of mass surveillance, and significant evidence of harm. Enabling ubiquitous mass surveillance requires maintaining an insecure Internet, which makes us all less safe from rival governments, criminals, and hackers.

Finally, Part Three outlines what we need to do to protect ourselves from government and corporate surveillance. The remedies are as complicated as the issues, and often require fine attention to detail. Before I delve into specific technical and policy recommendations, though, Chapter 12 offers eight general principles that should guide our thinking.

The following two chapters lay out specific policy recommendations: for governments in Chapter 13, and for corporations in Chapter 14. Some of these recommendations are more detailed than others, and some are aspirational rather than immediately implementable. All are important, though, and any omissions could subvert the other solutions.

Chapter 15 turns to what each of us can do individually. I offer some practical technical advice, as well as suggestions for political action. We're living in a world where technology can trump politics, and also where politics can trump technology. We need both to work together.

I end, in Chapter 16, by looking at what we must do collectively as a society. Most of the recommendations in Chapters 13 and 14 require a shift

in how we perceive surveillance and value privacy, because we're not going to get any serious legal reforms until society starts demanding them. There is enormous value in aggregating our data for medical research, improving education, and other tasks that benefit society. We need to figure out how to collectively get that value while minimizing the harms. This is the fundamental issue that underlies everything in this book.

This book encompasses a lot, and necessarily covers ground quickly. The endnotes include extensive references for those interested in delving deeper. Those are on the book's website as well: www.schneier.com/dg.html. There you'll also find any updates to the book, based on events that occurred after I finished the manuscript.

I write with a strong US bias. Most of the examples are from the US, and most of the recommendations best apply to the US. For one thing, it's what I know. But I also believe that the US serves as a singular example of how things went wrong, and is in a singular position to change things for the better.

My background is security and technology. For years, I have been writing about how security technologies affect people, and vice versa. I have watched the rise of surveillance in the information age, and have seen the many threats and insecurities in this new world. I'm used to thinking about security problems, and about broader social issues through the lens of security problems. This perspective gives me a singular understanding of both the problems and the solutions.

I am not, and this book is not, anti-technology. The Internet, and the information age in general, has brought enormous benefits to society. I believe they will continue to do so. I'm not even anti-surveillance. The benefits of computers knowing what we're doing have been life-transforming. Surveillance has revolutionized traditional products and services, and spawned entirely new categories of commerce. It has become an invaluable tool for law enforcement. It helps people all around the world in all sorts of ways, and will continue to do so far into the future.

Nevertheless, the threats of surveillance are real, and we're not talking about them enough. Our response to all this creeping surveillance has largely been passive. We don't think about the bargains we're making, because they haven't been laid out in front of us. Technological changes occur, and we accept them for the most part. It's hard to blame us; the

changes have been happening so fast that we haven't really evaluated their effects or weighed their consequences. This is how we ended up in a surveillance society. The surveillance society snuck up on us.

It doesn't have to be like this, but we have to take charge. We can start by renegotiating the bargains we're making with our data. We need to be proactive about how we deal with new technologies. We need to think about what we want our technological infrastructure to be, and what values we want it to embody. We need to balance the value of our data to society with its personal nature. We need to examine our fears, and decide how much of our privacy we are really willing to sacrifice for convenience. We need to understand the many harms of overreaching surveillance.

And we need to fight back.

—Minneapolis, Minnesota, and
Cambridge, Massachusetts, October 2014