Introduction

"Any sufficiently advanced technology is indistinguishable from magic."

Arthur C. Clarke, Report on Planet 3, *Technology and the Future*, 1972.

My wife and I took a long vacation in the summer of 2015, nearly three months in England and France. We rented cars, bought train tickets, and reserved hotels in big cities and cottages in the middle of nowhere, all entirely through web sites. We used online maps and Google Street View to scope out neighborhoods and attractions before finalizing our lodgings. While we were away, we used mobile phones to navigate unfamiliar places, we kept in touch with friends and family by email and Skype, we sent frequent pictures and occasional movies, and I worked for a few hours almost every day on a book with my co-author in New York. I even checked mail once or twice a day while we were on a ship in the middle of the Atlantic.

To which you are probably thinking, "So what? Doesn't everybody?" And except maybe for the unusually long vacation and the ship, you're right. This is standard operating procedure in today's world. It's almost magical how easy and convenient it is to make arrangements without intermediaries and to keep in touch even when far away from home. These technological systems are so commonplace that we tend not to think about them, even though they have changed our lives remarkably quickly.

My wife and I didn't use Airbnb to find places to stay, though we could have. Airbnb was founded in 2008; it now operates in 190 countries and has one and a half million listings. Airbnb has had a major impact on the hotel industry in many cities—its prices are often lower and its use of technology sidesteps an established regulatory environment that has been slow to adapt.

We also didn't use Uber since we only took a couple of cab rides, but we could have (and our London cabbie moonlighted as an Uber driver). Uber was founded in 2009; it operates in over 60 countries. Uber is having a significant impact on the taxi industry in many cities—as with Airbnb, its prices are often lower, and its use of technology also skirts a regulatory environment that has been slow to adapt.

We didn't use WhatsApp to keep in touch because Skype was better for us, but we could have. WhatsApp was also founded in 2009, and was acquired by Facebook in 2014 for $19 billion. It's the largest instant messaging system for phones, with over 900 million users. Late in 2015 and again in May and July 2016, a judge in Brazil ordered WhatsApp to suspend its service, because it had refused to comply with a court order to turn over data that was part of a criminal investigation. An appeals court quickly reversed the order each time and 100 million Brazilian users went back to using WhatsApp instead of the established phone companies.

These stories, which are far from unique, remind us of the range of technology, how quickly it changes, how disruptive it can be, and how deeply it has become part of our lives, making them better in all kinds of ways.

But there's a darker side to the story, not so cheery and optimistic. For every kind of interaction I just mentioned, countless computer systems were quietly watching and remembering—who you and I dealt with, how much we paid, and where we were at the time. A large part of this data gathering is for commercial purposes, since the more that companies know about us, the more accurately they can target us for advertising. Most readers know that such data is collected, but I expect that many would be surprised by how much and how detailed it is.

And as we learned not long ago, companies are not the only observers.

The NSA emails, internal reports, and PowerPoint presentations disclosed by Edward Snowden revealed much about spying in the digital era. The gist is that the NSA spies on everyone on a grand scale. Fearing for his own safety, Snowden provided material very cautiously to a small number of journalists in Hong Kong, then fled to Moscow, where he remains under the protection of the Russian government. Variously called a traitor and a hero, he's likely to be there for a long time. The story of how he got the information and safely revealed it is told in Glenn Greenwald's 2014 book *No Place to Hide* and Laura Poitras's movie *Citizenfour*, which won the 2015 Oscar for best documentary film.

Snowden's revelations were stunning. It was widely suspected that the NSA spied on more people than it admitted, but the extent surpassed everyone's imagination. The NSA routinely recorded metadata about all telephone calls made in the US— who called whom, when they talked, and for how long—and may have recorded the content of these calls as well. It had recorded my Skype conversations and email contacts, and probably the mail contents as well. (Yours too, of course.) It was tapping the cell phones of world leaders. It was intercepting huge amounts of Internet traffic by placing recording devices on equipment at various sites. It had enlisted or coerced the major telecommunications and Internet companies to gather and hand over information about their users. It was storing great amounts of data for extended periods of time, sharing some of it with spy agencies in other countries.

Meanwhile, back on the commercial front, hardly a day goes by when we don't learn of another breach of security at some company or institution, in which shadowy hackers steal information like names, addresses, and credit card numbers of millions of people. Usually this is criminal theft, but sometimes it's espionage by other countries, looking for valuable information. Sometimes foolish behavior by whoever maintains the information accidentally exposes private data. No matter what the mechanism, data that has been collected about us is all too often exposed or stolen,

potentially to be used against us.

So it's not all as wonderful and magical as one might think.

The purpose of this book is to explain the computing and communications technology that lies behind all of this, so you understand how such systems operate. How can pictures, music, movies, and intimate details of your personal life be sent around the world in no time at all? How do email and texting work, and how private are they? Why is spam so easy to send and so hard to get rid of? Do cell phones really report where you are all the time? How do iPhones and Android phones differ and why are they fundamentally exactly the same? Who is tracking you online and on your phone, and why does that matter? Can hackers take over your car? How about self-driving cars? Can you defend your privacy and security at all? By the end of the book, you should have a decent idea of how computer and communications systems work, how they affect you, and how you can strike a balance between using helpful services and protecting your privacy.

There are only a handful of fundamental ideas, which we will discuss in much more detail in the rest of the book.

First is the *universal digital representation of information*. Complex and sophisticated mechanical systems like those that stored documents, pictures, music and movies for much of the 20th century have been replaced by a single uniform mechanism. This is possible because information is represented digitally rather than in specialized forms like colored dyes embedded in plastic film or magnetic patterns on vinyl tape. Paper mail gives way to digital mail. Paper maps yield to digital ones. Paper documents are replaced by online databases. Different analog representations of information are replaced by a single digital representation.

Second is the *universal digital processor*. All of this information can be processed by a single general-purpose device, the digital computer. Digital computers that process the uniform digital representation of information have replaced complicated mechanical devices that process analog representations of information. As we'll see, computers are all equally capable in what they can compute, differing only in how fast they operate and how much data they can store. A smartphone is a computer of considerable sophistication, with as much computing power as a laptop from only a few years ago. Thus more and more of what might have been limited to desktop or laptop computers has found its way onto phones, and this process of convergence is accelerating.

Third is the *universal digital network*. The Internet connects the digital computers that process the digital representation; it connects computers and phones to mail, search, social networks, shopping, banking, news, entertainment, and everything else. You can exchange email with anyone, regardless of where they might be or how they choose to access their mail. You can search, comparison shop, and purchase from your phone, laptop, or tablet. Social networks keep you in touch with friends and family, again from phone or computer. There is great deal of infrastructure that makes all these services work.

An immense amount of *digital data* is also continuously being collected and analyzed. Maps, aerial photographs, and street-level views of much of the world are freely available. Search engines tirelessly scan the Internet so they can answer queries efficiently. Millions of books are available in digital form. Social networks

and sharing sites maintain enormous amounts of data for and about us. Online stores and services provide access to their wares while quietly recording everything we do when we visit them, aided and abetted by search engines and social networks. For all of our online interactions, Internet service providers log the connections we make, and perhaps more. Governments spy on us all the time, to an extent that would have been unbelievable only a decade or two ago.

All of this is changing rapidly because digital technological systems are getting smaller, faster, and cheaper at an exponential rate: every year or two, things are twice as powerful for the same price, or cost half as much as they did. New phones with fancier features, better screens, and more interesting applications arrive continuously. New gadgets appear all the time; the most useful ones often find their functionality subsumed into phones over time. This is a natural by-product of digital technology, in which any technological development leads to improvement across the board for digital devices: if some change makes it possible to handle data cheaper, faster or in larger quantity, all devices will benefit. As a result, digital systems are pervasive, an integral part of our lives both visibly and behind the scenes.

This progress must surely seem wonderful, and indeed in most ways it is. But there are clouds around the silver lining. One of the most obvious and perhaps the most worrying to individuals is the impact of technology on personal privacy. When you use your phone to search for some product and then visit store web sites, all parties keep records of what you visited and what you clicked on. They know who you are because your phone identifies you uniquely. They know where you are because phones report their locations *all the time*. With GPS, the Global Positioning System, the phone company can locate you to within five to ten meters; even without GPS, they know your location to within a hundred meters or so. And they can sell that information. Physical stores are increasingly watching you as well. Face recognition technology may well be able to identify you on the street or in a store. Traffic cameras scan your license plates and know where your car is. The tracking that we permit today without even thinking about it makes the monitoring in George Orwell's *1984* look casual and superficial.

The records of what we do and where we do it may well live forever. Digital storage is so cheap and data is so valuable that information is rarely discarded. If you post something embarrassing online or send mail that you subsequently regret, it's too late. Information about you can be combined from multiple sources to create a detailed picture of your life, and is available to commercial, government and criminal interests without your knowledge or permission. It is likely to remain available indefinitely and could surface to embarrass you at any time in the future.

The universal network and its universal digital information have made us vulnerable to strangers to a degree never imagined a decade or two ago. As Bruce Schneier says in his excellent 2015 book, *Data and Goliath*, "Our privacy is under assault from constant surveillance. Understanding how this occurs is critical to understanding what's at stake."

The societal mechanisms that protect our privacy and our property have not kept up with the rapid advances in technology. Thirty years ago, I dealt with my local bank and other financial institutions by physical mail and occasional personal visits. Accessing my money took time and it left an extensive paper trail; it would have been

difficult for someone to steal from me. Today, I deal with financial institutions mostly through the Internet. I can easily access my accounts, but unfortunately it's quite possible that through some blunder on my part or a screwup by one of these institutions, someone on the far side of the world could clean out my account, steal my identity, ruin my credit rating, and who knows what else, in no time at all and with little chance of recourse.

This book is about understanding how these systems work and how they are changing our lives. Of necessity it's a snapshot, so you can be certain that ten years from now, today's systems will seem clunky and antiquated. Technological change is not an isolated event but an ongoing process—rapid, continuous, and accelerating. Fortunately, the basic ideas of digital systems will remain the same, so if you understand those, you'll understand tomorrow's systems too, and you'll be in a better position to deal with the challenges and the opportunities that they present.