How often would you say you look at your smartphone every day? Your Facebook profile? Your Twitter account? Almost certainly more often than you’d think. The influence of the internet and the cloud on almost all areas of society is massive – and, mostly, inestimably beneficial. However, as these blinks will show you, there is a dark side to this force. It’s made possible hitherto unimagined forms of crime. And it isn’t just hackers in the murky waters of cyberspace that pose a threat to our integrity and safety. Companies like Google, Facebook and even Angry Birds play a role in this, too. That is, unless we read the fine print in the user agreements. But, honestly, when is the last time you read one of those? Luckily, there are other ways to protect ourselves. These blinks will show you how. In these blinks, you’ll learn

what Angry Birds knows about you;

why writing your novel in Google Docs might be a bad idea;

and why your city’s Sewer Department maybe shouldn’t be connected to the internet.

We’ve come a long way since the 1950s, when a single computer could barely fit inside a small building. Compare that with the world of today, where the iPhone in your pocket has more computing power than all of NASA during the Apollo 11 moon landing. But nowadays, technology is more than machines and gadgets. Rather, it’s an essential part of our lives – so essential, in fact, that over 80 percent of us check our phones within the first few minutes of waking up. And then we keep the same phones within three feet of us at all times. Our attachment to our phones can also be highly emotional. According to one US study, more than 90 percent of Americans feel high levels of anxiety if they forget their phone at home. Similarly, research from 2013 showed that Americans were spending more than five hours online every single day! We book our doctor’s appointments, check our bank statements and health insurance bills online, and browse Facebook and Amazon without considering the digital footprint we’re leaving behind. Often, our obsession with technology makes us forget that we’re putting our lives in the hands of software that can easily be hacked. This ignorance (or negligence) comes at a price. One study showed that, about 75 percent of the time, hackers successfully infiltrated the devices they attacked within mere minutes. This could in part be due to the fact that in 2015 “123456” and “password” remained the most popular passwords. To combat this, many companies have begun implementing multifactor authentication methods (e.g., using your password and a one-time code sent to you via SMS) to improve security. But you should nonetheless change your passwords regularly, keep them over 20 digits long and include numbers, symbols and spaces. Avoid being counted among the 50 percent of people who use the same password for all their online accounts.

We take our smartphones everywhere: to the toilet, to the gym and even to bed. You could say that our smartphones know us pretty well. They have plenty of data on our habits and our relationships, but how well is that data protected? As it turns out, you aren’t the only one with access to your personal information. In fact, your mobile phone acts a lot like a spy who knows exactly what you’re doing, where you’re doing it, who you’re doing it with, not to mention for how long and how often. For example, Google has developed technology that enables it to access calls made on your Android device, and use your conversation and the sounds around you to create targeted ads. Say you made a call while Usher was playing in the background; next time you googled something, an ad about his next concert might pop up. We’re mostly oblivious to all this data-gathering. A study done by Carnegie Mellon’s Human-Computer Interaction Institute revealed that only five percent of Angry Birds’ users

knew that the app collects locational data, which it then sells to advertisement companies. These companies then use this information as a forecasting tool to determine your future behavior and, thus, your purchases. In fact, according to a McAfee report, 82 percent of all Android apps check your online activities and 80 percent collect your location data without your permission. But should you care about location privacy? Who cares about your whereabouts anyway? In 2012 a Russian company launched an app called Girls Around Me that provided users with an interactive map displaying Facebook profile pictures, status updates and check-ins of the women in their proximity. The app was even approved by the Google Play and Apple App Stores! Is this social media or stalking? Whatever it is, it should be enough to make you think twice before skipping through the Terms of Service Agreement for your next app purchase.

So how is it that Google, Facebook, Twitter, YouTube and LinkedIn can all offer their services for free? Most people assume it’s because of the money they make from advertisements. But that’s only part of it. In actuality, you aren’t really their customer at all. Rather, you’re their product and primary source of income. Today, everything is connected via iCloud or Google products. But that convenience comes at a cost: our privacy. Just imagine all the intimate insights into your private life that you’ve unwittingly shared with Google: that time years ago when you googled “Symptoms of gonorrhea” or “Am I pregnant?” These searches didn’t fade with the passage of time. They’re still stored in a database somewhere, and could be used against you when you least expect it .That’s exactly what happened to British 26-year-old Van Bryan, who, before traveling to the US, tweeted to a friend that they should meet “before I go and destroy America.” Unfortunately, the US Department of Homeland Security didn’t appreciate the poetry of this party metaphor; they flagged him as a potential security threat and barred him and his partner from entering the United States. Very often we simply have no idea what kind of information we’re giving up and what it will be used for. That’s because terms and conditions, which outline that information, are designed such that we ignore everything on the page except “I Agree.” One day you might walk by a pharmacy and see a picture you took last summer of your child playing in the sand in an advertisement for children’s sunblock. If it’s on Instagram, it’s no longer yours. Similarly, all the documents you store on Google Drive belong to Google. If J. K. Rowling had written Harry Potter using Google Docs, she would have given Google the rights to the book and squandered her potential $15 billion fortune along with it.

Hacking has come a long way since 1971, when Apple founders Steve Wozniak and Steve Jobs hacked into phone networks and sold hacking devices called “blue boxes” to their fellow students at UC Berkeley. Nowadays, hackers understand that whoever possesses information has the upper hand in “the game.” Thanks to Edward Snowden’s leaks, we’ve learned that this is exactly what the National Security Agency (NSA) is after when spying on billions of people and leaders around the world – the upper hand. But the US government isn’t the only one trying to get their hands on information. In fact, in 2010 Google publicly admitted that hackers in China’s People’s Liberation Army had targeted their global Future Crimes password management system, thus granting them access to the accounts and web searches of millions of Google customers worldwide. Or consider another mass invasion of privacy that occurred in 2013, when the personal information from 110 million accounts was stolen from retail company Target’s database by a 17-year-old Russian hacker. As our data migrates away from physical silos into “the Cloud,” the need to protect our information becomes even more pressing. From a business perspective, the cloud seems like a great idea because of its implications for innovation, productivity and entrepreneurship. However, from the standpoint of public policy, security and law, problems such as privacy rights and the jurisdictional aspect of criminalizing hackers still need to be addressed. Questions like, “Where was the crime actually committed?” or “Where does the criminal operate from?” aren’t easily answered within the current legal framework. Thus, regular citizens share the responsibility of staying informed about cyber regulations. We must encrypt the data on our computers and phones with encryption programs, such as BitLocker and FileVault, and by keeping the operating system up to date.

We know the stereotype of a hacker: a 16-year-old computer whiz in a dimly lit room, hacking victims for the thrill of it. But according to a study by the Rand Corporation, 80 percent of hackers actually work for a company or government, and are closer to the age of 30. Indeed, cybercrime is much more organized, meaning we have to be extremely careful about what we post online. When you post about your upcoming vacation or weekend beach getaway on Facebook and Twitter, for example, you’re actually warmly inviting organized burglars to come and rob your home in your absence. Criminals have even used a website, PleaseRobMe.com, dedicated to this purpose. On it, they can window-shop for empty homes to ransack. And according to a 2011 study of convicted burglars in the UK, 78 percent admitted to having monitored Facebook, Twitter and Foursquare before choosing which house to rob.

Alternatively, hackers can also target you by examining the hidden data embedded in the pictures you post online, such as the GPS coordinates of where the picture was taken. So, think twice before showing off your new diamond ring or your plasma TV on Facebook for the world to see. Some people, distraught by how easily hackers can obtain their data, think that the solution is to get rid of these online profiles. But things aren’t so simple. Someone could easily create an online profile posing as you, and it’s far better that you control what sensitive information you post, rather than someone else. Just be careful about what you post on social networks, and consider the possibility that there will most likely be someone watching besides your Facebook friends. In addition to privacy issues, however, these new technologies have other, far-reaching effects. Our final blinks will look at how our reliance on the internet affects society as a whole.

Imagine a world where your alarm clock could connect with traffic cameras to adjust your alarm based on congestion estimates. Or where you didn’t need to ask your children whether they’d brushed their teeth because their toothbrushes would send a message to your phone once they had done it. While this may sound like a futuristic Hollywood movie, the technology is already here. In fact, Cisco has predicted that there will be 50 billion devices connected to the internet by 2020, compared to the 13 billion in 2013. The trend has been to connect any and all devices in the hope that it will make our lives easier. Many of us have already begun using RFID tags, wireless electromagnetic fields used to transfer data. We find these, for example, in our work ID tags that we use to get into our office or hotel buildings, in “wave and pay” credit cards and in the E-ZPass that we use to pay highway tolls.

In Australia, RFID tags are even used to monitor the location of 300 sharks off the coast. If they come too close to the beach, the chips implanted in their skin send an electronic signal that is turned into a tweet that warns tourists at the beach of possible danger. And that’s just the beginning. If we’re already vulnerable to cyber attacks through computers and phones, imagine having hundreds of hackable devices in your home. We’re only now learning that the cameras on our phones, computers, baby monitors and security systems could be streaming live to someone on the other side of the world, even when we think they are turned off. Luckily, this problem has a simple fix: when you’re not using your laptop’s camera, just stick a small Post-It on it to cover the lens.

While the internet has helped us to “modernize” our infrastructure, it has also put us at greater risk. Our railways, gas pipelines, 911-dispatch systems, air traffic controls, stock markets, drinking water, streetlights, hospitals, sanitation systems and electrical grids all depend on the internet to function properly. We have to ask ourselves: Is that a good idea? Hacking any of these critical infrastructural systems could have catastrophic consequences. Targeting a city’s electricity grid, for example, would leave that city in complete chaos. There would be no lights, no elevators, no ATMs. Garage doors wouldn’t open, traffic lights wouldn't work, air traffic control would be unable to contact the airplanes in the sky. There would be no cellphones and no internet. This happened in South Houston, where the Water and Sewer Department was hacked by an attacker who was traced to Russia using his IP address. Luckily, nobody got hurt, as he was only able to cause the water pumps to fail. But if he had mixed the wrong amount of chemicals to treat the water, he could have easily poisoned or even killed thousands of people. Clearly, connecting our infrastructure to the internet has some inherent dangers, and we should seriously consider whether it’s actually worth the risk. Consider our prison system. In California, for example, an alleged computer glitch in a program designed to ease overcrowding in many of the state’s prisons led prison officials to release 450 dangerous criminals on unsupervised parole. Then there’s the national Criminal Records Bureau, which admitted that more than 20,000 people had been criminalized due to errors in computer systems. Errors like this could damage your credit and prevent you from buying a car, a house or even from applying for a job. Even if you know you’ve filed your taxes correctly and on time, for example, an “error” could suggest that you committed tax evasion and ruin your life.

There’s no denying that newly emerging technologies such as robotics, artificial intelligence, genetics, synthetic biology, nanotechnology, and 3D printers will have an unimaginable impact on our lives. Whether these technologies will have a positive or negative effect on society depends much on who controls them. Ultimately, we decide what the consequences of this technology will be. Physicist Stephen Hawking and entrepreneur Elon Musk, for instance, have both argued that the rapid development of technology in areas such as artificial intelligence, nanotechnology and synthetic biology will forever alter humanity’s path. There will simply be no turning back. We have to decide how much of this technology we want in our lives. For instance, while having a driverless car sounds very enticing and fascinating, would you want to entrust the lives of your family to a car driven by a system that could easily be hacked?

Given the cyber threats we face every day, there are a few things you can keep in mind to make you less vulnerable to such attacks. For one, be mindful of the pictures you take, and, if you send them to someone, always encrypt them! For that matter, encrypt all of your data. Create a “guest” account on your computer, and use this account for your dayto-day use. Only use the “admin” account when updating programs from a trusted source. This will make it harder for malware and hackers to infiltrate your system. Next, turn off your computer when you are not using it. Do the same with Bluetooth, Wi-Fi and hot spots when you don’t need them. Finally, when you use your credit card or want to check your banking balance, only do it on your own device. Using a friend’s phone, or an airport or coffee shop network, will only put your data at greater risk!

The key message in this book: Modern technology and the internet have changed not only the way we interact with one another, but also the way criminals commit crimes. With so much of our information floating around on the net, and with so little prudence about what we share, we constantly put ourselves at risk.