Chapter 4: You’re Not the Customer, You’re the Product

GOOGLE

The gradual siphoning of your data begins innocently enough when you first start using Google to search the Web. You search, and it tracks and records the queries, not to mention every link you click on. From that initial search product, the carefully orchestrated acquisition of your personal information is carried out with artful precision. Eventually, a search engine wasn’t enough, and Google craved additional ways to gain further insights into you, your hopes, dreams, and desires. The result? Gmail. By providing a vast amount of storage space and a wonderfully seamless experience, Google gained access to both your personal and your professional e-mails. Now Google could understand not just your searches but everything you were writing and to whom. Google scanned and electronically read your messages and found new insights it could offer to advertisers, increasing its fees along.

Furthermore, “Don’t be evil” is Google’s official company motto. To allay any lingering doubts, Google’s icons and graphics, like its childlike multicolored logo and the adorable little green Android guy, were created to be so cute and nonthreatening that surely they could be trusted. Google Doodles, drawings on its home page celebrating everyone from Martin Luther King to Gandhi, further reassured the public that these were the good guys. Besides, Google had all these privacy policies too, which protect me, right? Not so fast. Viewed with a skeptical eye, Google creates products not to give you free e-mail but to get more data out of you. Like a pusher holding that first dime bag of heroin over a soon-to-be junkie, Google gave you something “on the house,” and only later might you realize the implications of the bargain you were making. By then, it was too late. This became clear when in early 2012 Google announced it was merging its data across all of its seventy products and services. The result: a unified, profound, and unprecedented view of you and your world.

Over the years, Google has introduced dozens of products that make our lives simpler and more productive. When it launched Gmail in 2004, it offered an amazing one gigabyte of data, vastly outmatching the paltry two megabytes offered by the dominant player of the day, Microsoft’s Hotmail. As the young organization hit its stride, other fantastic products emerged, and eventually we
were introduced to Google Calendar, Google Contacts, Google Maps, Google Earth, Google Voice, Google Docs, Google Street View, Google Translate, Google Drive, Google Photos (Picasa), Google Video (YouTube), Google Chrome, Google+, and Google Android, to name but a few. One by one, services such as phone calls, translation, maps, and word processing—services for which we would previously have paid hundreds of dollars (think Microsoft’s Office)—were now suddenly free.

The most benevolent interpretation of this bounty would be that Google was merely providing products the public wanted, satisfying our ever-growing technological needs (and those of advertisers). A less altruistic explanation might be that each and every one of the aforementioned products was created with the specific intent to trick, cajole, and coax users to reveal an ever-increasing volume of data about themselves and their lives ad infinitum.

Google to its credit provides mostly wonderful products that serve the needs of its users, and the company is filled with loads of extremely talented and dedicated employees. But make no mistake, its loyalty will always be first and foremost to its advertisers, who pay the bills, and to its shareholders, to whom it has a fiduciary obligation to extract from you (its product and supply chain) the maximum value possible. That is why Google stores every search you have ever conducted on the site indefinitely. Google does not forget, and Google does not delete. Each of the above queries is used to profile you, categorize you, and sell you to advertisers and data miners who make further assumptions about you based on your searches, e-mails, voice mails, photographs, videos, and locations as cataloged by Google. How many data is Google processing every day? you might wonder. About 24 petabytes’ worth (that’s 1 million gigabytes or 1,000 terabytes—a measure used to describe a volume of data). To put that in perspective, it takes approximately “1 gigabyte of data to store 10 yards of books on a shelf.” If all the data Google processed on a daily basis were printed and those books were stacked on top of each other, the pile of books would reach halfway from earth to the moon. That’s how much information Google is storing on users—every day!

Facebook is a marketer’s dream. Advertisers know every last intimate detail about a Facebook user’s life. Did you realize every time you speak a query into Apple’s Siri artificial intelligence agent, your voice recording is analyzed and stored by the company for at least two years?

**TERMS OF SERVICE**

According to a study at Carnegie Mellon University, the average American encounters 1,462 privacy policies a year, each with an average length of 2,518 words. If one were to read each and every one of those policies, it would take seventy-six full workdays, at eight hours a day, from our lives. We are just not going to read those. Anybody who uses Google Docs or happens to upload a
spreadsheet, PDF, or Word document to Google Drive automatically grants ownership of the document.

More recently, Facebook began to ask hundreds of millions of users of its mobile app to allow its new Photo Syncing option to automatically upload every image taken with your phone to the social network’s vast data servers. Once Facebook has been downloaded, users agree in the ToS to grant it permission to “take pictures and videos with the camera,” a setting that allows Facebook to turn on your mobile phone’s camera at any time without your confirmation.

**Chapter 5: The Surveillance Economy**

But “I have nothing to hide” is absolutely the wrong way to think about our new dataveillance society. It is a false dichotomy of choice: either we accept total surveillance, or we are criminals worthy of suspicion.

AT&T revealed that in 2013 it received more than 300,000 requests for data relating to both civil and criminal cases. The demands for information came from state, federal, and local authorities and included nearly “248,000 subpoenas, nearly 37,000 court orders and more than 16,000 search warrants. Central Intelligence Agency pays AT&T $10 million a year for its call data and suggested Verizon too supplies data to the U.S. government. The government now spends just “$574 per taxpayer, a paltry 6.5 cents an hour,” to track each and every American.

**Chapter 6: Big Data, Big Risk**

2014 each and every minute of every day, we

- sent 204,166,667 e-mail messages
- queried Google’s search engine 2 million times
- shared 684,000 pieces of content on Facebook
- sent out 100,000 tweets on Twitter
- downloaded 47,000 apps from the Apple App Store
- uploaded 48 hours of new video on YouTube
- posted 36,000 new photographs on Instagram

According to the National Crime Prevention Council, nearly half of all teens are affected by cyber bullying. For young people facing the persistent harassment, it seems as if there is no escape; as a result, a full 20 percent of middle school students admitted to “seriously thinking about attempting suicide” because of online bullying.

According to the Pew Research Center, today 95 percent of young people in the United States are online, and 74 percent of teens aged twelve to seventeen are mobile Internet users, often accessing the online world via cell phones and
Moreover, 95 percent of young people aged ten to twenty-three have at least one social media account. Much of this Internet access takes place outside the purview of their parents, 74 percent of whom say they are overwhelmed by modern technology and don’t have the energy, time, or ability to monitor what their children do online.

Chapter 7: I.T. Phones Home

Even worse, mobile phones may be the most insecure of all devices. The software is notoriously easy to subvert, the risks are poorly understood, and the systems for device protection are immature and wholly underdeveloped. As a result, smart phones are among the easiest devices to hack. Today, there are viruses and Trojans specifically designed to give attackers access to your cell’s microphone, recording any sounds nearby, even when you are not on a call. Anything you do or any data you store on your mobile phone—your entire text-messaging history, your address book, photographs, call logs, social networking passwords, and account information—can all be intercepted, hacked, and forwarded to criminal organizations for future exploitation.

Mobile phone malware can be used to track your persistent location and allow criminals to see your position in real time, conveniently plotted on a Google map.

Chapter 9: Mo’ Screens, Mo’ Problems

In a phenomenon known as swatting, bored hackers have been able to telephone police 911 emergency phone systems with spoofed telephone identities in order to report nonexistent crimes, resulting in the response of heavily armed police SWAT units. The FBI recorded at least four hundred incidents of swatting in 2013 alone.

If something is on a screen, whether it be a computer, iPad, industrial control system, street sign, GPS device, radar installation, or mobile phone, our first inclination is to trust what we see before us. However, we have shown time and time again that everything from our friends on Facebook to the numbers we dial on our mobile phones can be rigged to deceive us. The problem is that we are leading lives fully intermediated by screens and other technologies that, although they give the appearance of transparency, are in fact programmed, controlled, and operated by others.

Chapter 10: Crime, Inc.

In total, organized crime is believed to account for up to 15 to 20 percent of global GDP.

While historically perhaps 80 percent of hackers were independent freelancers, today the opposite is true. According to a 2014 study by the Rand Corporation, a
full 80 percent of hackers are now working with or as part of an organized crime group.

Chapter 11: Inside the Digital Underground

Nearly 20 percent of American and EU citizens have been the victims of identity theft.

In the same way our every move online can be tracked, recorded, sold, and monetized today, so too will that be possible in the near future in the physical world. Real space will become just like cyberspace, and as all the objects around us join the Internet of Things (IoT), any meaningful distinction between the online and the off-line worlds will disappear. With the widespread adoption of more networked devices, what people do in their homes, cars, workplaces, schools, and communities will be subjected to increased monitoring and analysis by the corporations making these devices. Of course these data will be resold to advertisers, data brokers, and government alike, providing a heretofore-unprecedented view into our daily lives. Unfortunately, just like our social, mobile, locational, and financial information, our IoT data will leak, providing further profound capabilities to stalkers and other miscreants interested in persistently tracking us.

In late 2013, Google sent a letter to the Securities and Exchange Commission noting, “we and other companies could [soon] be serving ads and other content on refrigerators, car dashboards, thermostats, glasses, and watches, to name just a few possibilities.”

Chapter 13: Home Hacked Home

Ford Motors, admitted in early 2014, “[We know] everyone who breaks the law, we know when you’re doing it. We have GPS in your car, so we know what you’re doing.

Chapter 16: Next-Generation Security Threats: Why Cyber was Only the Beginning

As narrow AI (Artificial Intelligence) capabilities grow, we are seeing algorithms play increasingly active roles throughout more and more businesses and professional settings:

• algorithmic criminal justice (red-light and speeding cameras determine infractions of the law)
• algorithmic border control (an AI can flag you and your luggage for screening)
• algorithmic credit scoring (your FICO score determines your creditworthiness)
• algorithmic surveillance (CCTV cameras can identify unusual activity by computer vision analysis, and voice recognition can scan your phone calls for troublesome keywords)
• algorithmic health care (whether or not your request to see a specialist or your insurance claim is approved)
• algorithmic warfare (drones and other robots have the technical capacity to find, target, and kill without human intervention)
• algorithmic dating (eHarmony and others promise to use math to find your soul mate and the perfect match)
• algorithmic trading on Wall Street (bots carry out stock buys and sells)

Each algorithm is saturated with the profound human bias of the person or people who wrote the formula.

Chapter 17: Everything’s Connected, Everyone’s Vulnerable: Here’s What You Can Do About It

Do the following things and avoid more than 85 percent of the digital threats that pervade our lives daily.

- Update Frequently
- You should absolutely not use the same password for several different sites. Passwords should be long (think twenty digits or more) and contain upper- and lowercase letters, as well as symbols and spaces
- Download software only from official sites
- Pay close attention to apps and their permissions. They are “free” for a reason and you’re paying with your privacy. If a flashlight app tells you it needs access to your location and contacts, run the other way.
- Turn off your computer when you aren’t using it
- Back up your data frequently
- Always use a password on your mobile phone, and consider enabling biometric security, such as Apple’s Touch ID fingerprint technology
- Encrypt
  - keeping Wi-Fi on allows retailers and advertisers to persistently track you through your physical world
  - turn off services and connections on your smart phone when you aren’t using them