

CHAPTER 4

You're Not the Customer, You're the Product

The truth will set you free, but first it will piss you off.

GLORIA STEINEM

Parkinson's, relapsing remitting multiple sclerosis, necrotizing fasciitis, acute lymphocytic leukemia, childhood-onset diabetes, HIV, amyotrophic lateral sclerosis—a diagnosis of any one of these diseases would undoubtedly strike fear in the hearts of most patients receiving such life-altering news. In years past, individuals with such illnesses would have found themselves depressed and alone, unable to discuss their plight with others who knew exactly what they were going through. Moreover, the paucity of comprehensible medical information written for actual human beings would have further isolated these patients from friends and family. That is why Jamie and Ben Heywood (whose brother was diagnosed with Lou Gehrig's disease) founded the Internet site PatientsLikeMe.com—to allow visitors to share their stories and connect with others going through the exact same health trials and tribulations. Since the site's founding in 2004, it has grown to a global community of more than 200,000 patients diagnosed with fifteen hundred unique diseases. For thousands of people, PatientsLikeMe.com has been both a figurative and a literal lifesaver, as users learned more about their illnesses and exchanged survival strategies and treatment protocols in a variety of online discussion forums.

It was that opportunity to connect with others that first drew Bilal Ahmed, a thirty-three-year-old businessman from Sydney, Australia, to the site. Ahmed had been suffering from anxiety and depression since the death of his mother, and he found it difficult to discuss his condition with friends and family. Ahmed created a pseudonym account on PatientsLikeMe and joined its Mood Forum, where users share intimate details about emotional disorders such as bipolar disease, PTSD, bulimia, addiction, OCD, and thoughts of suicide. On the Mood Forum, he dutifully listed his symptoms, test results, and all the drugs he had been prescribed to treat his depression. There he connected with other patients around the world, formed friendships, and shared the most intimate of details regarding his illness on the password-protected site—receiving exactly the type of support he had yearned for.

It was for that reason that Ahmed felt so violated after having been notified by PatientsLikeMe of “unauthorized activity” on its Mood Forum discussions board. At 1:00 a.m. on May 7, 2010, system administrators noticed suspicious activity coming from several new accounts that were “scraping,” that is, copying every single message off the private online forum and downloading the information to a third-party site. PatientsLikeMe eventually identified the intruder responsible for the break-in: the Nielsen company, the same advertising giant known for TV’s Nielsen ratings. A Nielsen subsidiary known as BuzzMetrics admitted taking the data, which it added to its online collection of information purloined from the other 130 million blogs, eight thousand message boards, Twitter, Facebook, and other social media sites it tracked. Nielsen sells these data to advertisers, marketers, and, in this case, major pharmaceutical houses as raw material in a multibillion-dollar global data-mining industry.

Nielsen’s egregious activity, though ethically repugnant, was technically legal under current federal law, and on May 18, 2010, PatientsLikeMe disclosed the incident to its entire user community. The company also took the opportunity to remind users of its own privacy policy terms and conditions:

We take the information patients like you share about your experience with the disease and sell it to our

partners (i.e., companies that are developing or selling products to patients). These products may include drugs, devices, equipment, insurance, and medical services . . . [Y]ou should expect that every piece of information you submit (even if it is not currently displayed) may be shared.

Wait, what? The note disclosing the Nielsen break-in was bad enough, but the follow-up e-mail detailing the Web site's privacy policy was a massive wake-up call. For most users of PatientsLikeMe, it was the first time they realized that all the medical information that would previously have remained securely locked in the filing cabinet of their doctors' offices—their conditions, diagnosis dates, family histories, symptoms, CD4 counts, viral loads, lab results, biographical information, gender, age, photographs, and even entire genetic sequences—was now being sold by PatientsLikeMe, the very place these desperate patients had trusted to help them and to protect their information.

Though PatientsLikeMe claimed it only sold de-identified/anonymized data on its patients, new and emerging data companies such as PeekYou LLC of New York had long ago worked out a variety of patentable techniques to match people's real names to the pseudonyms they used on blogs, chat forms, and Twitter. In other words, any pharmaceutical company or health insurer that wanted the information from PatientsLikeMe need only hire PeekYou to reverse engineer your user name or pseudonym en masse to fully identify you. For Bilal Ahmed, this meant that all of the personal data he had entrusted to PatientsLikeMe were now owned by Nielsen/BuzzMetrics. In a public interview after his identification, Ahmed noted he felt totally violated by the incident and immediately deleted all his posts from the site as well as the list of drugs he had been prescribed, but by then of course it was too late. Every time he and other patients had posted highly detailed accounts of their illnesses and symptoms on PatientsLikeMe, there were companies like Nielsen lurking in the background scraping up all the data he shared. Those that weren't siphoned off by third parties were freely sold by PatientsLikeMe itself, disclosed in the

fine-print privacy policy that Ahmed and so many others failed to ever read when they created their accounts.

As Ahmed discovered, social networks are the new public records. All that you share, wittingly or not, is being scraped, sorted, and warehoused by newly emerging global data behemoths and sold to advertisers, governments, and third-party data brokers, each with an increasingly voracious appetite to know the most intimate details of your life. These data can be used to determine if you have any preexisting conditions, if you should pay higher life insurance rates, or if you should be denied a job or promotion. While sharing may be caring, it also could mean higher insurance rates. As a result, the hundreds of thousands of people using PatientsLikeMe learned a valuable if painful lesson: they were not in fact the Web site's customers; they were its product, sold to the highest bidder in an effort to drive the company's own bottom line.

Our Growing Digital World—What They Never Told You

By 2013, Americans were spending more than five hours a day online with their digital devices. We read the news on Web sites run by CNN, the *New York Times*, and ESPN. We check our bank balances at Citibank and Wells Fargo. We shop at Amazon and Macy's. We pay our ConEd and Comcast bills, make appointments with our doctors, and check our health insurance with Blue Cross. We watch *House of Cards* on Netflix and *Downton Abbey* on Hulu. And that's just the beginning. Take a moment to think about how you used your smart phone today. Eighty percent of us check our mobile phones for messages within fifteen minutes of waking up. Did you provide a quick status update today to your friends on Facebook? You'll probably get a "Like" or two or maybe a funny comment from a friend. And what about those selfies you sent your boyfriend? The Internet has become a vast and free treasure trove of information and entertainment, and so we dutifully gorge ourselves at the trough. And at every step of the way, we are collectively leaving behind a daily digital exhaust trail big enough to fill the Library of Congress many times over. How all these data are cre-

ated, stored, analyzed, and sold are details that most of us readily gloss over, but do so at our own peril.

There is no denying the power of social media. In a mere ten years since its creation in 2004, Facebook sprinted from zero to 1.3 billion members around the globe. Each day, more than 350 million photographs are uploaded, while the omnipresent Like button is pressed approximately six billion times. Social media chronicle our dates, graduations, home purchases, childbirths, new pets, marriages, and divorces. They also can be instruments for geopolitical change, as was seen during the 2010 Arab Spring, when a Google executive named Wael Ghonim created a Facebook page to highlight the slaughter of a young Egyptian protester at the hands of Hosni Mubarak's internal security forces. "Two minutes after he started his Facebook page, 300 people had joined. Three months later, that number had grown to more than 250,000." Similarly, Twitter, Google, and other services were credited with helping to drive change in Tunisia, Iran, and Libya. While history will judge the role social media played in the Arab Spring, there is no doubt these services can be a force for good.

And the allure of these tools is clear. After all, most of us spend our lives trolling the Web for music, recipes, investment advice, news, directions, business opportunities, celebrity gossip, and sports scores. When we're not checking e-mail, we're playing *Temple Run* or *Fruit Ninja*. And it's all entirely free of charge. Even the fees we once paid to travel agents, newspapers, and music companies have all but disappeared—eliminated thanks to the generous people who brought us the World Wide Web. But did you ever stop and wonder why Google never sends you a bill?

Ask the average person why Google, Facebook, Twitter, YouTube, and LinkedIn are free, and he or she may be a little fuzzy on the details. Many think it has to do with advertising—that is, those annoying banner ads or pop-up screens with which we are constantly barraged. Perhaps, but that is only a small part of the story. Others may believe the trade-off to be pretty simple. These companies give us valuable services for free, such as e-mail, news, videos, and a place to post pictures, and in return we give them a little bit of information about ourselves. Occasionally, we need to watch an advertisement that has been specifically designed to

suit our needs, but privacy settings put us in the driver's seat and nobody gets hurt, right? If only it were that straightforward. The reality of the bargain we've made is much more disconcerting.

Take Google as an example, a company founded in 1998 by two Stanford PhD students, Larry Page and Sergey Brin, in a friend's garage in Menlo Park, California. The pair invented a groundbreaking algorithm that vastly improved search results on the nascent World Wide Web and attracted a loyal following drawn in by their simple interface and high-quality search results. In 2000, they began selling ad keywords for particular products aligned with any given search phrase. For example, if your query was "Paris, France," you would be served up sidebar ads for Air France, travel insurance companies, or Hilton Hotels. Companies looking for new customers could now market via Google's keyword ads with previously unknown precision, getting a much better return for their advertising dollars. What started as a humble idea by two Stanford students in 1998 had by 2015 grown into a global juggernaut.

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. People

might balk if they fully understood the true nature of the exchange. So, to paraphrase Otto von Bismarck, it's best for Google's customers if they don't see or know quite how the sausage is made. But pulling back the curtain and studying the sausage factory are fundamental in order to understand an ever-growing mountain of data security risks facing our world today.

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 the way as it refined its profile of you. If you wrote an e-mail to your mom telling her you were sad over a recent breakup, Google might suggest an antidepressant, a comedy club, or a Caribbean vacation. As long as you remained logged in to Gmail, it could track all of your searches to your unique identifier with the company; as a result, Google's profile of you grew richer, as did the company.

When Google offered you the opportunity to store your contacts online, it in turn could evaluate the size, strength, and purchasing power of your social network. When Google introduced its Maps program and provided gratis GPS and driving directions, it could now track the places you went. Google wondered whom you were calling and created Google Voice to find out. Not only could it now track every one of your telephone calls, but it would transcribe your voice-mail messages using voice-recognition and voice-transcription software. A very cool technical feat at the time, it also allowed Google to understand what you and your interlocutors were discussing. If somebody left you a voice-mail message suggesting Italian food for dinner, Google would sell that informa-

tion to its advertisers, and suddenly ads for pizza would show up across your Google world. For further precision, Google created the Android operating system (OS) and gave it away for free. In exchange, Google could now track you anywhere and everywhere you took your smart phone.

Of course if Google told you all this, you might be freaked out, so instead a pretty ruse was created, a fig leaf of sorts. When Google was founded, it projected itself as the underdog, the little guy battling evil Microsoft. In fact, Google would tell its users that it was so benevolent that it decided to make "Don't be evil" its 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. Previously, your searches in Google, what you did on your Android phone, and the videos you watched on YouTube were data that *in theory* Google held separately. Not anymore; now Google has a single unified, highly detailed picture of you and everything you do across its Googleverse. Many have even argued that Google knows you better than you know yourself. It is precisely because it has all of these data that it can command top dollar from advertisers for your information.

If it wasn't abundantly clear previously, you are not Google's customer; you are its product. That's why you don't get a bill. That's why there's no 800 number for technical support. Those items are reserved for its real customers: the advertisers who are purchasing

all the data you litter along Google's information superhighway. You are the thing Google sells to other people; that's the deal it never quite made truly clear to you, and whether or not you realize it, you are completely complicit in the process.

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: "the Ohio State college Republicans" you asked about ten years ago, the "symptoms of gonorrhea" after that one-night stand, the "Girls Gone Wild videos" while traveling for work at your hotel, "is my husband gay?" when feeling dejected and lonely.

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!

With all of these data come immense insights and tremendous power, but as the old saying goes, power corrupts. Around the world, Google has been repeatedly sued for privacy violations, security breaches, mishandling user data, theft of intellectual property, tax evasion, and contraventions of antitrust laws. After a lawsuit by thirty-eight American state attorneys general in 2013, Google admitted that its bizarre-looking Street View cars, those outfitted with high-tech 360-degree roof cameras, were not just taking photographs for its Street View mapping product as they

drove down the streets of our neighborhoods but also pilfering data from computers inside our homes and offices, including passwords, e-mails, photographs, chat messages, and other personal information from unsuspecting computer users.

In October 2013, a federal judge refused to dismiss a class-action lawsuit against Google claiming its practice of reading and scanning users' Gmail accounts violated U.S. laws against unlawful interception and wiretap. Before that, in 2012, Google was fined a record \$22.5 million by the Federal Trade Commission when it was revealed it routinely circumvented privacy settings on Apple computers and for those using Apple's Safari Web browser to track users across the Web against their clearly stated wishes.

Of course Google is a highly innovative company, and in its quest to coax ever more data out of you for its real customers (advertisers), Google has planned a host of new products that may make past privacy concerns pale by comparison to future ones. One such product is Google Glass—a wearable computer in the shape of a pair of eyeglasses sporting an “optical head-mounted display” that connects to the Internet and is capable of projecting visual information onto a screen embedded in the glass. The device runs on the Android operating system and can take photographs and video and stream them in real time via its built-in camera and microphone.

In early 2014, Google Glass was the subject of a *Simpsons* episode titled “Specs and the City” in which all of Mr. Burns's employees were given a pair of “Oogle Goggles.” On the show, Homer Simpson and his colleagues use the glasses to see new information about the things and people around them. Ominously, perhaps presciently, Mr. Burns, while seated in his office command center, is able to access the glasses of all his employees and see what they are viewing and doing in real time (in an effort to reduce theft of office supplies).

Even the former head of the Department of Homeland Security (DHS) Michael Chertoff has raised privacy and public policy concerns about Google Glass. He rightfully asked who owned the users' video data and whether the entire video database would be mined and analyzed for commercial purposes. One could also legitimately ask about government access to these data, either ret-

respectively or in real time, for reasons ranging from crime fighting to "national security." Consider the implications for a moment. By using Google Glass, are you granting the company the right to capture all the live-streaming moments of your daily life, everything you see and hear, so that it can sell these data to advertisers? For example, if, while you were wearing the glasses making your morning coffee in your bathrobe, the Google Glass vision algorithm recognized the object in your field of view as a coffee pot (entirely possible), might you start seeing coupons for Starbucks on your eyeglass screens? Given the aforementioned privacy violations we've seen from the search giant, what else might it be capable of as we enter the age of wearable surveillance?

The Social Network and Its Inventory—You

Of course Google is not alone in its business model of selling you to its advertisers, and there are thousands of companies around the world that do the exact same thing, including most notably Facebook. Founded by Mark Zuckerberg in his dorm room at Harvard in 2004, Facebook is the iconic Silicon Valley success story. With more than 1.2 billion monthly active users, Facebook is by far the largest social network in the world. It has succeeded by getting people to talk about themselves in ways never previously imagined. Sexual orientation, relationship status, schools attended, family tree, lists of friends, age, gender, e-mail addresses, place of birth, news interests, work history, catalogs of favorite things, religion, political affiliation, purchases, photographs, and videos—Facebook is a marketer's dream. Advertisers know every last intimate detail about a Facebook user's life and can thus market to him or her with extreme precision based upon the social graph Facebook has generated.

Moreover, Facebook created a variety of innovations that allow it to track users across the entirety of the Web, including via its omnipresent Like button. You've been trained to click on the cute little blue thumbs-up button to express your support for a particular idea, status update, or photograph; after all, it's the polite thing to do. Your friends see that you support their message, but what neither of you sees is what happens with the data generated with

each and every Like—data that are captured, dissected, and sold to marketers and data brokers around the world. When you use Facebook's ubiquitous log-in credentials to visit other sites on the Web, such as Spotify and Pandora, Facebook's data-mining engine is crunching your preferences for Lady Gaga over Blake Shelton, just as it is tracking all the Web sites you visit with the Facebook icon on them (even if you don't log in).

In case you aren't sharing enough, Facebook is happy to create new rules and regulations to force you to share more, as it did in 2012 when it instituted its mandatory timeline "feature." The change provided advertisers a dynamic, ever-updating window into your life's interests at any moment in time and more fodder for Facebook to sell to advertisers. Facebook, like Google, has been broadly criticized on issues including privacy, child safety, and hate speech. It has been sued repeatedly around the world, most recently in U.S. federal court in San Jose, California, for regularly and "systematically intercepting users' private messages . . . and sharing the data with advertisers and marketers."

Of course, Google and Facebook are by no means alone in getting you to reveal personal data about yourself and selling them: so too are Twitter, Instagram, Pinterest, and hundreds of other firms. For example, 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? The question, however, is not who is storing your data—everybody seems to be these days—but what are they doing with the information? If the Faustian bargain were as simple as we provide you cool services "for free" in exchange for a few data, all would be fine in the world. But things are not so simple, and as you will soon see, keeping and storing these massive volumes of data in a world that is so connected, dependent, and vulnerable puts you at risk in ways you might never have imagined.

You're Leaking—How They Do It

Every time you visit a modern Web site, the site places invisible digital marking files known as cookies on your computer or phone's

hard drive. With these tiny computer files, it becomes possible to track you and your activities across the Web. In addition, all your digital devices have their own unique fingerprints that allow you to be traced, shadowed, and cataloged. Unique identifiers, such as the Internet protocol (IP) address for the computer network you use to access the Internet, the media access control number (MAC address) from your Wi-Fi network cards, and the IMEI or IMSI number from your mobile phone, all allow online companies to know exactly what devices (and users) are utilizing their services.

All of these data are tracked, unified, and exploited to give Internet companies and their advertisers a clear and persistent look into you and your online activities. According to a 2012 *Wall Street Journal* study, one of the fastest-growing businesses today is spying on Internet users. In its report, it highlighted fifty of the most popular Web sites and discovered that on average each left more than 64 cookie tracking files for advertisers to trace and surveil your online activities. The Web site with the most tracking software was Dictionary.com with a total of 234 tracking files implanted on your computer with every visit. All of these tracking beacons and cookies are combined with your Likes, pokes, and tweets to paint an eerily detailed picture of the digital you. Accordingly, your computer's cookies transform themselves into cookie monsters, revealing data you never intended to become public.

Not only are you leaking data as a result of your own social networking activities, but your friends and family are leaking data about you as well. Every time a colleague puts your name and address into his Google Contacts or iPhone, he is providing Google and Apple with your personal details. Record a birthday in Microsoft's Outlook calendar for your nephew, girlfriend, or business colleague, and Microsoft now knows the person's date of birth. When your friends tag you at a party on Facebook (after you called in sick to work), they have shared your location with marketers and potentially the rest of the world, including your boss. Social media and Internet companies love when users do this work for them; it's like having free code monkeys completing survey after survey feeding their big-data machine.

This even happens when your friend uses a particular Internet site or service that you don't. For example, for those who do not

have a Gmail account but whose friends do, sending an e-mail to any one of Gmail's 425 million users means that Google has now become a party to your conversation. So if you use your university or work e-mail address to send your sister a message on her Gmail account, and even though you never opened a Google account yourself, Google will still read, scan, and search the message for words of interest that it can sell to advertisers—a practice for which it is now being sued in federal court. In its defense motion for the case filed with Judge Lucy Koh, Google shockingly claimed “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” In other words, Google’s argument is that by e-mailing any Gmail user, you have automatically waived any privacy rights and consented to its seizure and sale of your e-mail message and its contents, even if you intended the message to be private and don’t have a Gmail account yourself.

It’s not just your friends who are leaking data about you to third parties such as Google but also your children. In fact, sites aimed at children install more tracking technologies on computers than those for adults. Though a federal law titled the Children’s Online Privacy Protection Act limits the information online marketers can collect on kids under thirteen, the rule is blatantly violated on a routine basis. Children are repeatedly presented with requests to sign up for contests, play games, and fill out online questionnaires in an effort to elicit more and more data about them, in contravention of federal law. Well-known companies such as McDonald’s, General Mills, Viacom, Turner Broadcasting System, and Subway have all been fined for coaxing data out of young kids on their highly cartoon-ified Web sites such as HappyMeal.com, ReesesPuffs.com, Nick.com, and SubwayKids.com. In another case, Sony BMG Music asked minors to enter their street addresses and phone numbers on fan pages for their favorite bands, information that Sony then sold to data brokers on at least thirty thousand occasions, without first obtaining parental consent as required by federal law. But why would venerable companies like McDonald’s, Google, Facebook, General Mills, and Sony commit acts such as these? Simply stated, there are vast sums of money at play, and you and your data are worth the risk to them, given the exorbitant rewards.

The Most Expensive Things in Life Are Free

The business proposition that most Internet users do not understand is that they are indeed paying for all of the so-called free services they receive online—and paying dearly. That sucking sound you hear is your privacy, your data, and all of the details that make up your unique identity being inhaled by the giant Internet vacuuming system. The details of your searches—stuff you wouldn't dream of sharing with your closest friends and family—are being filtered into a big computer algorithm in the sky, aggregated into petabytes, and sold for billions. That is why you have free search and Google has a \$400 billion valuation. Because of you—its product. That's the deal you've made, whether you realize it or not.

Google's consolidated revenue for 2013 was more than \$59 billion. That amount is the difference between how much your privacy is worth to Google's advertisers and how much you are not being paid. Google gets \$59 billion, and you get free search and e-mail. A study published by the *Wall Street Journal* in advance of Facebook's initial public offering estimated the value of each long-term Facebook user to be \$80.95 to the company. Your friendships were worth sixty-two cents each and your profile page \$1,800. A business Web page and its associated ad revenue were worth approximately \$3.1 million to the social network.

Viewed another way, Facebook's billion-plus users, each dutifully typing in status updates, detailing his biography, and uploading photograph after photograph, have become the largest unpaid workforce in history. As a result of their free labor, Facebook has a market cap of \$182 billion, and its founder, Mark Zuckerberg, has a personal net worth of \$33 billion. What did you get out of the deal? As the computer scientist Jaron Lanier reminds us, a company such as Instagram—which Facebook bought in 2012—was not valued at \$1 billion because its thirteen employees were so “extraordinary.” Instead, its value comes from the millions of users who contribute to the network without being paid for it. Its inventory is personal data—yours and mine—which it sells over and over again to parties unknown around the world. In short, you're a cheap date. You've happily provided Internet companies everything you know, everything

you do, and everywhere you go in exchange for a modicum of convenience or entertainment.

As if that cash-for-data deal weren't stark enough, Google has decided to grow its \$400 billion valuation by using you and your photographs in its advertisements. In October 2013, the company announced a new feature, called shared endorsements, that began to appear in search, map, and Google Play store results. So if, for example, you rated a song five stars in Google Play's music store or gave a +1 thumbs-up of support to your local bar or bakery, Google now granted itself the right to sell your likeness, name, and endorsement to ad firms and data brokers. This way when your friends Charlie and Juanita searched for a bar or a song in Google, they would see your shining face endorsing the product next to their search results. George Clooney and Angelina Jolie get paid for their celebrity endorsements; do you?

Google introduced "shared endorsements" after a highly controversial similar program called Sponsored Stories was established by Facebook in which the company used your Likes to endorse its true customers—advertisers and the products they represented. After a class-action lawsuit was filed against Facebook, the social network ended the controversial feature, but not before earning \$230 million in the eighteen months that the program ran. In the end, Facebook settled the lawsuit for \$20 million, or about two cents for each of its users. Right about now you may be asking yourself, "But how can they get away with this?" The answer is simple: you said they could.

Terms and Conditions Apply (Against You)

**"I have read and agree to the Terms of Service"
is the biggest lie on the Web.**

TERMS OF SERVICE: DIDN'T READ, [HTTP://TOSDR.ORG](http://TOSDR.ORG)

We've all seen them. Those impossibly long, fifty-page disclaimers written in four-point font, single-spaced, with one-eighth-of-an-inch margins. They are designed to be impossible to read—so we don't. We don't read them, we don't understand them, and for this we pay a heavy price. In today's world, terms of service (ToS) are

attached to every Internet site, mobile phone contract, cable TV subscription, and credit card. They delineate how all your private data can be sucked away from you and used in ways unimaginable—including many that we would object to, if only we could actually understand the agreement we were making.

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. In the aggregate, that works out to 53.8 billion hours for all Americans, at an estimated national opportunity cost of \$781 billion of lost productivity every year because of the nightmare and disgrace that are the ToS.

Of course if this were just a story about lost productivity, it might not be so egregious, but these policies directly affect your wallet as well. A study in the *Wall Street Journal* estimated that the completely one-sided language in the ToS policies costs each American household \$2,000 a year—for a total of \$250 billion annually—money that we are cheated out of as a result of a deck of cards that is entirely stacked against us. Though companies call these policies terms of service, for consumers they would be much more aptly described as “terms of abuse.”

Let's just take one example of what it is costing you to use a social media site, in this case, LinkedIn, whose privacy policy states,

You grant LinkedIn a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicenseable, fully paid up and royalty-free right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to LinkedIn, including, but not limited to, any user generated content, ideas, concepts, techniques and/or data to the services, you submit to LinkedIn, without any further consent, notice and/or compensation to you or to any third parties. Any information you submit to us is at your own risk of loss.

So by using LinkedIn, you are granting it irrevocable and perpetual access (for free) to any information you have ever listed on the site; there's no take backs, no do overs. Once it has your data, social network graph, work history, skills, and education, it can sell them now or in the future in any way it desires, including in ways not yet discovered (for example, to own perpetual holographic rights to use your images in advertising?). To demonstrate how ridiculous privacy policies have become of late, the British retailer GameStation ran an experiment to see if anybody ever read its ToS. The company amended its privacy policy to read,

By placing an order via this GameStation Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant us a non transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions.

That's right, seventy-five hundred GameStation customers who purchased something on its site for the one day it ran the experiment irrevocably granted their immortal souls to the U.K. online retailer. While the point was irreverently made, ToS are no laughing matter, and courts around the world have found your click to be legally binding, with significant financial, privacy, and security implications for you.

Nearly all Internet companies have similarly draconian policies that work against you. While most stop just short of claiming rights to your immortal soul, many come pretty close, and the more words they use, the worse it is for you. Facebook's privacy policy has grown from 1,004 words in 2005 to 9,300 words by 2014 (not counting links to various sub-policies, terms, and conditions). To put that in perspective, Facebook's privacy policy is more than twice as long as the U.S. Constitution. Meanwhile, PayPal's privacy policy and amendments are the longest in the

industry at 36,275 words. By comparison, Shakespeare's *Hamlet* has 30,066 words, including the famous 'To be, or not to be' soliloquy and the moving 'Good night, sweet prince' speech at the end." Complicating matters further, Facebook and others grant themselves full rights to change their privacy policies at will and do so frequently.

Worse, many companies make the privacy settings nearly impossible to access and understand—Facebook alone has fifty different privacy settings with 170 options, well beyond the understanding of the average human being—and that's the point. Moreover, even if you did spend the hours it might take to customize the privacy options to your liking, any updates by Facebook to its ToS automatically put all users back to the default settings, which are the maximum level of openness (so it can sell more of its product—you—to its actual customers, advertisers). Unless you frequently check the settings—as you should—you will find that Facebook has en masse disregarded your explicit previously established privacy wishes. As a result, Facebook reserves for itself the power to monetize you without interference or cacophony from its assembly line of noisy human products.

Three months after it was purchased by Facebook, Instagram outraged its users when it announced it would sell their names, images, and photographs to advertisers. According to its updated ToS, Instagram argued that parents who had uploaded photographs of their minor children had implicitly consented to the use of the images in advertisements. The picture of your infant you uploaded to share with your parents could now be used to sell baby food because Instagram had granted itself those rights. Your brilliant shot of the sun setting over Manhattan? It could be sold as stock imagery for newspapers and magazines. As a result of its change in ToS, sixteen billion user photographs now became Instagram's intellectual property, explaining why Facebook paid \$1 billion for a company with thirteen employees.

Google too has demonstrated its penchant for ridiculous ToS. For example, anybody who uses Google Docs or happens to upload a spreadsheet, PDF, or Word document to Google Drive automatically grants ownership of the document to Google. According to Google's ToS,

When you upload or otherwise submit content to our services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify and create derivative works, such as those resulting from translations, adaptations or other changes and license to communicate, publish, publicly perform, publicly display and distribute such content.

Think about that. If J. K. Rowling had written Harry Potter in Google Docs instead of Microsoft Word, she would have granted Google the worldwide rights to her work, the right to adapt or dramatize all the Muggles as Google saw fit, to say nothing of the Hogwarts School of Witchcraft and Wizardry. Google would have retained the rights to sell her stories to Hollywood studios and to have them performed on stages around the world, as well as own all the translation rights. Had Rowling written her epic novel in Google Docs, she would have granted Google the rights to her \$15 billion Harry Potter empire—all because the ToS say so.

That Facebook, Google, Twitter, and others all store your online data and monetize it to the fullest extent possible should be of little surprise by now. What might surprise, however, is the growing number of platforms from which advertisers can collect and process this information, including the formerly humble telephone. Alexander Graham Bell would be shocked to see how his invention had been transformed into the smart phones and apps of today, each reaching deeper and deeper into our lives, with notable risks to both our privacy and liberties.

Mobile Me

Right, my phone. When these things first appeared, they were so cool. Only when it was too late did people realize they are as cool as electronic tags on remand prisoners.

DAVID MITCHELL, *GHOSTWRITTEN*

There are currently more mobile phones on the planet than there are people, and as a result an omnipresent digital skin has begun to

envelop the earth, with consequences for all. Today's smart phones are powerful miniature computers that we carry with us 24/7 and have become an indispensable part of our lives. Sixty-three percent of Americans admit to checking their phones every hour, and nearly 10 percent check every five minutes. These devices are taken to the bathroom, to the gym, and to our beds. Mobile phones and tablets have replaced our cameras, computers, calculators, calendars, address books, radios, televisions, and games. In fact, making calls is only the fifth most common activity for which people use their smart phones, after Web browsing, social networking, playing games, and listening to music. These gadgets form an integral part of our lives, and 84 percent of us admit that we could not go a single day without our mobiles. Smart phones serve as our trusted companions and as such have unlimited access to our day-to-day lives. But has this access been granted without sufficient consideration of what it means to be virtually conjoined with a computer we carry on our person round the clock?

For as ubiquitous and useful as mobile phones are, they are also veritable snitches in our pockets, digital spies tracking our every move. That device in your purse or jeans that you think is a cell phone is in reality a beacon, constantly signaling the world and providing an incessant stream of data about you, your location, and your life's activities. In the United States alone, mobile phones generate about 600 billion unique data events every day, including where you were, whom you texted, and the photographs you uploaded. The volume of data we leak via our home and work computers pales in comparison with what we're leaking through our digital pals in our pockets. Mobile phones provide the clearest picture into any one person's habits and preferences, and indeed into his or her life. So who has access to all these data? Many more people than you realize. Knowing your physical location, where you spend your time and money and with whom, provides greater opportunities to mine you ever more deeply for monetizable information. Data brokers, spies, and criminals too have come to view the cell phone as a rich fountain of intelligence for their targeting purposes. As a result, they, like others, are all going after the smart phone with a vengeance.

The opportunity to own all your mobile data was the reason Google created its Android mobile phone operating system and

gave it away to developers and users for free. But as we've seen previously, free can be a very expensive proposition. The Android mobile phone software provides Google with your mobile phone number, network information, device storage data, call logs, and contacts lists, plus access to a bevy of new sensors that can detect your motion, location, and even ambient temperatures, humidity, and sound levels.

Given all these new technological hooks into your life, Google lost no time in filing a patent application for what it called "Advertising based on environmental conditions." *Ka-ching!* Now Google can detect if you are in a hot location and accordingly serve up an ad for air-conditioning or ice cream. Using its ambient sound technology, Google could also listen in on your phone calls for background noise and then serve up ads based on those preferences. So if you listen to Usher in the background while talking to Aunt Margaret on your Android phone, Google has the ability to detect that and show you ads for his upcoming concerts the next time you check your Gmail or search the Web.

Facebook too has now added the ability to use your phone's microphone to listen in on you and the ambient sounds nearby—all agreed to in the updated ToS and part of its big push for mobile users. When Facebook revealed in the fourth quarter of 2013 that it had reached 945 million monthly mobile users and that 53 percent of its revenue was now coming from mobile ads, the market showered its love on the company, adding billions of dollars to its valuation in the days following the announcement. By finally creating its own mobile app for users, Facebook devised not only a better user experience but also a new tool for grabbing voluminous amounts of data from a user's mobile device.

Pilfering Your Data? There's an App for That

An Apple iPhone commercial in 2009 famously introduced us to the phrase "there's an app for that" as a means of demonstrating there is an iPhone application for every possible human need. A bold statement at the time, but perhaps Steve Jobs was right. Since its launch in 2008, there have been more than sixty-five billion

downloads from Apple's App Store, generating revenues of over \$10 billion in 2013 alone. To compete with Apple, Google launched its own app store known as Google Play, and each company hosted more than a million separate applications available for download. The growth rate of these small software programs known as apps has been phenomenal, but what motivates tens of thousands of developers around the world to create apps? Money of course, but how do they make money when the majority of apps are free? Well, as we've seen before, free is a great business model, as long as you are monetizing people by commandeering their personal data in volumes. As it turns out, apps are a brilliant ecosystem for doing just that. It also helps to explain why companies like Rovio (maker of the wildly popular game *Angry Birds*) have grown from near obscurity to a \$9 billion valuation in just a few years.

In the same way that cigarettes are nothing more than efficient nicotine-delivery systems, apps are nothing more than efficient and streamlined tools for the transmission of your private data to advertisers (though cigarettes are at least regulated). The amount of information siphoned off your mobile phone by apps is staggering. For example, the mere act of downloading the Facebook app to an Android phone automatically shares the phone's number with the social network—even before a user has signed into the service for the first time or even agreed to the ToS. 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. The social network's ToS also allows it to read your text messages. 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.

Though Facebook maintains it isn't really turning on your camera or reading your texts, it has reserved for itself the right to do so. But frankly, how does any user actually know what data are being taken from the phone: it's all done in the background, hidden in the underbelly of the app, and not meant to be seen by those Facebook is productizing.

The appropriation of your personally identifiable information (PII) occurs the moment you agree to download an app. For example, when you buy an Android app in the Google Play store, Google provides the app company with your complete name, your e-mail address, and where you live. This occurs without any clear warning every single time you download an app. But who exactly are these app companies—thousands of them located around the world—who now have your name, address, and phone number? What are their privacy policies, and what do they do with this information? How securely do they store it, and to whom are they selling it? The fact is, it's the Wild, Wild West out there, and there is little or no regulation that effectively protects you and your data from these third-party information hawkers. By sharing millions of names and contact details with its app vendors, Google increases the likelihood that your data will leak, be stolen, or be misused.

As you probably now suspect, Zynga's wildly popular Facebook games *FarmVille*, *Texas Hold 'Em Poker*, and *Mafia Wars* are free of charge because they, too, have been tapping into your PII, including the names of all your Facebook friends. This information is sold to dozens of advertising and Internet-tracking companies, even if you have your privacy settings set to maximum protection. While putting birds in slingshots and shooting them at egg-thieving pigs can certainly be fun, as attested to by the one billion people who have downloaded the *Angry Birds* app, the game has a ravenous ability to collect its users' personal information, including all locations they travel with their mobile phones. And yet, a study by Carnegie Mellon's Human-Computer Interaction Institute revealed that only 5 percent of *Angry Birds* users knew that the company was storing their locational data in order to track them in the real world for targeted advertising purposes. But *Angry Birds* is far from the only offender. McAfee reported that 82 percent of Android apps track your online activities and an astounding 80 percent collect location information.

Location, Location, Location

For advertisers, there are three key questions: Who will buy their products, what are customers looking for, and where are they? In

the online world, Google won the “what” question long ago with its powerful search algorithms. Google knows what you are looking for and will even fill out the search box at the top of your screen before you’ve finished typing your own query. Facebook knows “who”—it knows you and your social network in greater depth than any other firm. But “where”—where is not yet owned by any single company, and a battle is brewing among existing titans and a breed of new start-ups looking to definitively own where. Serving you up an ad or coupon for frozen yogurt just as you are approaching a Pinkberry is akin to advertising nirvana. Until now, the technology to do this was lacking, but that has changed because of the mobile phone revolution, and thus the gold rush for your locational data is on. McKinsey has estimated the market value of your personal location data to be more than \$100 billion to the retail, media, and telecommunications industries over the next ten years.

“Where” is determined by a number of techniques—by your phone’s GPS antenna, by triangulating your mobile’s location and distance between cell-phone towers, and even by the Wi-Fi networks you connect to. These locational data are increasingly being appended to more and more of your online transactions in so-called file metadata—that is, data that provide data about other information. For example, when most people take a photograph with their mobile phones, their locational data (GPS coordinates, longitude and latitude, and so forth) are embedded in the image file. When you upload those photographs and videos to Craigslist, Flickr, YouTube, Facebook, and hundreds of other services, those revealing locational metadata can be passed right along with the original file. For some apps, the request for your location is perfectly logical, such as with Google Maps or GPS navigation tools. But for others, capturing your locational data is just another way for app makers to sell your data at greater value.

Your postings on Facebook, your tweets, and your searches on Yelp all use locational data. Moreover, there are an increasing number of location-based service (LBS) start-ups that are incorporating your “where” into everything from shopping to real estate. Perhaps one of the fastest-growing niches in LBS apps are those involving romance and love, especially “love” of decidedly limited duration. Apps like Tinder and Grindr have been downloaded millions of

times and may be responsible for more than fifty million hookups, according to Tinder's CEO. Ah, love apps . . . a many-splendored thing.

But with all the potential benefits of these new streams of locational data come new risks as well. In 2012, a Russian company launched an app called Girls Around Me, which was approved for inclusion in both the Apple App Store and Google Play. Girls Around Me took advantage of all those public postings, status updates, photographs, and check-ins with locational metadata that women had been posting on services like Facebook and Foursquare. When a user launched the Girls Around Me app on his phone, he need only press a single button to be presented with an interactive map showing the faces of young women in his vicinity and their exact locations. Using the app's "radar mode," anybody could geo-locate these women and see their Facebook profiles.

For example, if a man used Girls Around Me and saw that a young attractive woman had just checked in at the local Starbucks, he could track her, access her Facebook profile, see what high school or college she had attended, learn that she recently vacationed in Las Vegas, and find out the names of her parents, her favorite drink, and the fact that earlier that day she had watched *Orange Is the New Black* on Netflix. Armed with this information, the man, a stranger, could casually walk up to the woman as she stood in line ordering her daily grande extra-hot soy latte and strike up a conversation discussing how much he loved Vegas and *Orange Is the New Black*. A very useful tool for dating, as well as for stalkers and rapists searching for women of interest.

For advertisers, "where" is not just about your current location; it's also about where you were yesterday and last month and where you are likely to be tomorrow. Locational records detail exactly how much time you spend in Macy's versus Best Buy, and the sequence of these movements tell much more. In today's world of location-based advertising, when a woman takes her smart phone and its apps with her to the gynecologist's office, an interesting data point is registered across the mobile advertising ecosystem. But when the same woman three weeks later walks into a Babies "R" Us, a much deeper truth is potentially revealed. By aggregating your locational data over time, advertisers can deduce whether you

go to church or synagogue, work out at a gym, drink often at the local bar, see a psychologist, or are cheating on your spouse. But who exactly are these people collecting all of this information, how much of it do they have, and what do they do with it? As you are about to discover, vast amounts, growing at an exponential rate for uses we and they haven't even begun to identify.