Privacy Is Power

Why and How You Should Take Back Control of Your Data

CARISSA VÉLIZ

BANTAM PRESS
If you are reading this book, you probably already know your personal data is being collected, stored, and analysed. But are you aware of the full extent of privacy invasions into your life? Let's start at dawn.

What is the first thing you do when you wake up in the morning? You probably check your phone. Voilà: that is the first data point you lose in the day. By picking up your phone first thing in the morning you are informing a whole host of busybodies – your smartphone manufacturer, all those apps you have installed on your phone, and your mobile company, as well as intelligence agencies if you happen to be an ‘interesting’ person – what time you wake up, where you’ve been sleeping and with whom (assuming the person you share your bed with keeps his phone near him too).

If you happen to wear a smart watch on your wrist, then you will have lost some privacy even before you wake up, as it records your every movement in bed – including, of course, any sexual activity.1 Suppose that your employer gave you that watch as part
of a wellness programme to encourage healthy habits that can lead to cheaper insurance premiums. Can you be sure that your data will not be used against you? Are you confident your employer will not see it? When your employer gives you a device, they remain its legal owner – be it a fitness tracker, a laptop, or a phone – and they can access the data from that device at any time without your permission.

After checking your heart rate during the night (way too fast – you need to exercise more) and sending that data to your smartphone, you get out of bed and brush your teeth with an electric toothbrush. An app lets you know that you have not been brushing as often as you should.

You have overslept this morning, and your spouse has already left for work. You go to the kitchen and look for sugar for your coffee, only to realize you’ve run out. You decide to ask your neighbour if she has some to spare. Standing outside her door, you notice something unusual about it – there’s a camera. When she opens the door, she explains: it’s a new smart doorbell. If it’s a Ring doorbell, a company owned by Amazon, Ring employees will probably review that video footage of you in order to tag objects manually in an effort to train software to perform recognition tasks. These videos are stored unencrypted, making them extremely vulnerable to hacking. Amazon has filed a patent to use its facial recognition software on doorbells. Nest, owned by Google, already uses facial recognition in its cameras. In some cities like Washington DC, the police want to register, and even subsidize, private security cameras. It is anybody’s guess where footage from smart doorbells is going to end up and what it will be used for.

Your neighbour doesn’t have sugar – or maybe she doesn’t want to give you any after you sneered at her new doorbell. You are forced to settle for unsweetened coffee. You turn on the TV (a smart TV, of course) to distract yourself from its bitter taste. Your favourite TV show is on – that guilty pleasure you would never admit to watching.

You get a call. It’s your spouse. You mute the TV.

‘Why are you still at home?’

‘How did you know?’

‘My phone is connected to our smart meter. I could see you were using electricity.’

‘I overslept,’ you say.

He doesn’t sound very convinced by your explanation, but he has to go.

You wonder whether this is the first time you have been spied on through your smart meter. Smart meters are not only a privacy risk with respect to the people you share your home with. They are notoriously insecure devices. A criminal can hack yours, see when you’re away from home, and rob your property. Furthermore, data from smart meters is held and analysed by energy service providers. Some of this data can be quite sensitive. For example, your energy footprint is so precise that it can reveal which television channel you are watching. The data can then be sold or shared with interested third parties.

Your teenage son suddenly walks in and interrupts your thoughts. He wants to talk to you about something. Something sensitive. Perhaps it’s about a problem related to drugs, or sex, or bullying at school. You don’t turn off the TV. It remains muted, playing images in the background. Your smart TV is probably collecting information through a technology called ‘automatic content recognition’ (ACR). It tries to identify everything you watch on TV, and sends the data to the TV maker, third parties, or both. Researchers found that one Samsung smart TV had connected to more than 700 distinct internet addresses after being used for fifteen minutes.
That's the least of it. If you had time to read the privacy policies of the objects you buy, you would have noticed that your Samsung TV included the following warning: 'Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party.' Even when you think you've turned your TV off, it might still be on. Intelligence agencies like the CIA and MI5 can make your TV look as though it is off while they record you.

After your son has shared his most intimate thoughts with you, your TV manufacturer, and hundreds of unknown third parties, he leaves for school, where he will be forced to lose yet more of his privacy through the school's surveillance of his internet use. You un mute the TV. Commercials are on. You think that you're finally going to get a moment of privacy. You're wrong. Unbeknown to you, inaudible sound beacons are being broadcast through those TV (and radio) commercials as well as through music in shops and are being picked up by your phone. These audio beacons function like sound cookies that allow businesses to triangulate your devices and purchasing habits through location. That is, they help businesses track you across different devices. Thanks to this ultrasonic cross-device tracking, a company can make sure that the person who sees a particular ad for a product in the morning on TV, and looks it up on her laptop an hour later, then buys it at the shop in her neighbourhood, or orders it online.

You receive another call. This time it's a colleague from work.

'Hey, I'm not sure how this happened, but I just received a recording of a very private conversation you were having with your son. It seems that your digital assistant Alexa sent it.'

You thank him for letting you know and hang up, wondering whether Alexa might have sent that conversation to other people in your contact list. Furious, you get in touch with Amazon. They explain: 'Echo probably woke up to a word in your conversation that sounded like "Alexa". Then, it thought you were saying "send message". It must have asked "To whom?" and whatever you were saying then was interpreted as a name.' Sometimes smart speakers are activated by hearing a television show in which a word is spoken that is similar to their wake word. If you were to have your television on all day, that would happen between one and a half and nineteen times per day (not counting the times when the actual wake word is said on television). When Alexa sent the private conversation of a user in Portland, Oregon, to a random contact, the user vowed never to plug in the device again. You go a step further and smash the Echo against the wall. Your spouse will not be happy about that.

You are very late for work now. You get in your car and drive to your office. You bought your car second hand from an acquaintance. It probably never crossed your mind, but it turns out that that person has access to your data, because she never disconnected her phone from the car app. Furthermore, your carmaker is gathering all kinds of data about you – the locations you visit, the speed you drive at, your music tastes, your eye movements, whether your hands are on the wheel, and even your weight as measured by your seat – that can end up in the hands of your insurance company, among other third parties.

You get to work. You live in London, and your office is in Westminster. As you pass the Houses of Parliament, data from your phone may be vacuumed up by IMSI-catchers – fake cell phone towers that trick mobile phones into connecting to them. Once connected, IMSI-catchers collect identification and location data. They also allow eavesdropping on phone conversations, text messages, and web browsing. There is evidence that this equipment is being used by the police in London to spy on people, for example,
at peaceful protests and near the UK Parliament. Popular advice given online to protect your privacy includes leaving your phone at home when going to a protest. Though they are mostly used by governments, IMSI-catchers can be used by anyone, since they are sold by private companies and can also be home-built.

While the data on your phone is being hoovered, you step into your office. A colleague greets you and looks at his watch, making it clear that your tardiness is being noted. You sit in front of your computer and try to inhale deeply, but you lose your breath at the sight of hundreds of unread emails. You open the first one. It's from your boss. 'Hey, I noticed you weren't in the office this morning. Will you have that report I asked for ready on time?' Yes, you will, but you wish your boss weren't breathing down your neck.

The next email asks you to fill in anonymous evaluations of your co-workers. Your boss is a firm believer in work surveillance. You know that he tracks your every movement, keeping tabs on whether you attend meetings, seminars, and even informal dinners and drinks after work. You know he monitors your social media because he has warned you in the past about posting political content. You feel queasy at the thought of evaluating your co-workers and being evaluated by them.

Then there's an email from your favourite shoe brand. You might think it harmless to your privacy to receive emails, but about 70 per cent of commercial emails and 40 per cent of all emails contain trackers. Opening an email allows third parties to track you across the web and identify you as one and the same user across devices. Trackers can be embedded in a colour, a font, a pixel, or a link. Even ordinary people are using trackers to know whether their emails are being read, when, and where. Given that trackers can reveal a person's location, stalkers can use them to find you.

The next email is from your brother. He has used your work address even though you have asked him not to. Employers, including universities, have access to your emails - one reason among others never to use your work email for personal purposes. In his email, your brother informs you that he received a direct-to-consumer genetic testing kit as a birthday present and went ahead and tested himself. You might be happy to learn, he writes, that our family is 25 per cent Italian. The bad news is that he has a 30 per cent chance of getting heart disease; given that he is your brother, that probably applies to you too. You reply: 'I wish you had asked for my consent. Those are my genes too, and those of my child. Didn't you know our grandmother was Italian? If you want to know more about our family, ask me.'

Worried about your genetic data, you look at the privacy policy of the company your brother used. It doesn't look good. Testing companies can claim ownership of the DNA sample you send them, and use it in whichever way they want. Privacy policies of DNA testing companies usually refer to the 'de-identification' or 'pseudonymization' of information to reassure people. Genetic data is not easy to de-identify effectively, however. It is in the nature of genetic data that it can uniquely identify individuals and their family connections. Replacing names with randomly generated ID numbers does not provide much security against re-identification. In 2000, computer scientists Bradley Malin and Latanya Sweeney used publicly available healthcare data and knowledge about particular diseases to re-identify 98 to 100 per cent of individuals on an 'anonymized' DNA database. You wonder what will become of your brother's genetic data, and whether it will ever count against you or your son if you apply for insurance or a job, for example. The worst part of it is that home genetic tests are incredibly imprecise. About 40 per cent of
results are false positive. Your brother may have given away all of the family’s genetic privacy in exchange for mumbo jumbo that will nonetheless be treated as facts by insurance companies and others.

It’s time for a work videoconference with a client, who has requested you connect through Zoom. Many people hadn’t heard about Zoom before the coronavirus pandemic, when it became the most popular videoconferencing app. You’ve had bad experiences with it before, like the time you sent a ‘private’ text chat to your colleague making fun of the way a client was dressed only to realize your client received all texts in a transcript at the end of the call. You avoid the chat now. During the pandemic, you were also horrified to learn that every word spoken during your calls and every document shared became part of Zoom’s data collection.

You have a vague idea that Zoom has improved its privacy and security policies now, but can you trust a company that claimed to implement end-to-end encryption when it didn’t?

When the call is over, in an effort to relax you log on to Facebook. Just for a little while, you tell yourself. Perhaps the photos of your friends’ good times will cheer you up (they won’t). Given that you suspect your boss monitors what you do on your computer, you use your personal phone.

Facebook has violated our right to privacy so many times that a comprehensive account would merit a book in itself. Here I mention only a few ways in which it invades our privacy.

Everything you do while on Facebook gets tracked, from your mouse movements to the things you write and decide to delete before posting (your self-censorship). You start browsing the section entitled ‘People You May Know’. This feature has been crucial in expanding Facebook’s social network, which went from 100 million members when the tool came out in 2008 to over 2 billion in 2018. Among the people you can see there you may recognize distant relatives, or people you went to school with. That doesn’t sound too bad. I suggest you don’t go much deeper into that rabbit hole though. If you do, you may likely find that Facebook is trying to connect you with people you do not want to connect with.

Some connections between people are problematic, like when the real identities of sex workers are outed to their clients. Or when a psychiatrist’s patients get linked together, throwing medical confidentiality out of the window. The psychiatrist in question was not friends with her patients on Facebook, but her patients probably had her in their contact books. Among many other ill-fated connections, Facebook has also suggested as friends a harasser to his (previously anonymous) victim, a husband to his wife’s lover, and a victim to the man who robbed her car.

Facebook’s current mission statement is to ‘give people the power to build community and bring the world closer together’. What about giving people the power to disconnect from toxic or undesirable relationships? ‘Bringing the world closer together’ sounds cozy until you ask yourself whether you want closeness forced upon you with people you fear, dislike, or want to keep at a distance for professional or personal reasons.

Facebook has proved its lack of respect for privacy in many other ways. About 87 million Facebook users had their data analysed for political purposes by the data firm Cambridge Analytica. In 2018, 14 million accounts had personal data stolen in a hack.

For years, Facebook allowed Microsoft’s Bing search engine to see Facebook users’ friends without their consent, and it gave Netflix and Spotify the ability to read and even delete Facebook users’ ‘private’ messages. In 2015, it started logging all text messages and calls from Android users without asking for their consent.

Facebook has probably used facial recognition on your photos
without securing proper consent from you. When Tag Suggestions asked you ‘Is this Jack?’ and you responded ‘yes’, what you did was give away your labour for free to train Facebook’s facial recognition algorithm. Facebook has filed patents that describe systems to recognize shoppers’ faces in stores and match them to their social networking profiles. To top it off, Facebook asked users for their telephone numbers as a security measure, and then used that information for its own purposes – to target ads and unify its data sets with WhatsApp, its messaging app. In 2019, hundreds of millions of Facebook users’ phone numbers were exposed in an open online database, because the server they were on was not password-protected. These are just some of the latest disasters, but the full list is a long one, and everything seems to indicate that Facebook’s violations of our right to privacy are not about to stop.

Facebook may seem like a social network on its surface, but its real business is trading in influence through personal data. It is more of a personalized advertisement platform than a social medium. It is willing to go to great lengths to scrape up as much personal data as possible with as little friction as possible so that it can sell advertisers access to your attention. Judging by its history, if it can get away with it – and so far it has – Facebook will not ask for consent, it will not make an effort to investigate who is getting your data and how it is being used, and it is willing to break its promises. Protecting your privacy seems to be the lowest priority on its list. And you can’t even stay away from this data-hungry monster, because Facebook has a shadow profile on you even if you are not a user. It follows you around the web through its pervasive Facebook ‘like’ buttons, even if you don’t click on them. It’s no wonder a British parliamentary report has suggested that Facebook has behaved like a ‘digital gangster’ in the past few years.

After browsing Facebook for a while and feeling ‘creeped out’ about the friends it suggests and the ads it shows you, you take a break from it. You try to get down to some work, but you cannot concentrate, thinking about how your boss is likely monitoring every move you make on your computer. Luckily for you, it’s time for lunch. Except you’re not hungry, so you decide to go to a nearby shop to buy something for your son that may help him feel better.

You go into a clothing shop to find a shirt. Bricks-and-mortar businesses have felt disadvantaged in comparison to online shops because the latter were the first to collect oceans of data from customers. So physical shops are trying to catch up. The shop you enter uses technology that identifies you as a returning shopper through your Wi-Fi mobile signal. Mobile devices send unique identification codes (called media access control – or MAC – addresses) when they search for networks to go online. Shops use that information to study your behaviour.

Not content with that, shops may also use cameras to collect data on you. Cameras may help to map customers’ paths and study what people are attracted by, how they navigate the shop. Cameras have become so sophisticated that they can analyse what you are looking at and even what mood you’re in based on your body language and facial expression. The shop may also be using facial recognition. Among other uses, facial recognition allows businesses to cross-reference your face with a database that looks for a match with past shoplifters or known criminals.

You step out of the shop and check your phone. An alert reminds you that you have a doctor’s appointment. There’s a health issue that has been bothering you for some weeks. You’ve searched online, trying to find a solution, and hoped it might go away on its own, but it hasn’t. You haven’t told anyone in your family so as not to cause unnecessary worry. Our search engines know more about
us than our spouses: we never lie to them or conceal our worries from them.

You go to the doctor. You receive a notification while you are in the waiting room. Your sister has posted the latest photo of your baby niece. Her chubby hands make you smile. You make a mental note to warn your sister about the dangers of exposing her kids online. You ought to tell her that our online photographs are being used to train facial recognition algorithms that are then used for all sorts of nefarious purposes, from the surveillance of vulnerable populations by authoritarian regimes to outing pornography actors and identifying strangers on the subway in Russia.48 But your niece’s irresistible smile distracts you. Pictures of her are sometimes the highlight of your day, and the kind of thing that makes the data economy bearable, even when you know that engaging content such as endearing babies is precisely what the data vultures feed on.

A nurse announces that the doctor is ready to see you. As your doctor asks sensitive questions, records your answers on her computer, and schedules some tests for you, you wonder where that data might end up. Your medical data is often for sale. Data brokers49 — traders in personal data — can acquire medical data from pharmacies, hospitals, doctors’ offices, health apps, and internet searches, among other sources. Your medical details could also end up in the hands of researchers, insurance companies, or prospective employers.50 Or the NHS (the UK’s National Health Service) may decide to donate your records to a company such as DeepMind, owned by Alphabet (Google’s parent company). The transfer of data may be done without your consent, without you benefiting from such an invasion of privacy, and without any legal guarantee that DeepMind will not link your data to your Google account, thereby further eroding your privacy.51

You could also be the victim of a data breach. In 2015, over 112 million health records were breached in the United States alone.52 You could even become the victim of extortion. In 2017, criminals got access to medical records from a clinic and blackmailed patients; they ended up publishing thousands of private photos, including nude ones, and personal data including passport scans and national insurance numbers.53

As these thoughts race through your mind, you feel tempted to lie to your doctor about sensitive information that (you hope) is not necessary to get an accurate diagnosis. You may even feel encouraged not to get the prescribed tests done at all, even though you need them.

After the doctor’s, you go back home to pack for your work trip to the United States. All day you have been tracked by the apps on your phone. If you allow location services to be on so you can receive local news, the local weather, or other similar information, dozens of companies receive location data from you. In some cases these apps update and receive your location data more than 14,000 times a day. Location-targeted advertising is a business worth an estimated $21 billion.54

Among the many hands that are trading your location data around are telecoms. Jealous of Silicon Valley’s business success, telecoms are eager to compete in the data trading market.55 Your mobile phone is constantly connecting to the nearest cell phone tower. As a result, your mobile service provider always knows where you are. Mobile networks not only sell location data to other companies; journalists have exposed that at least some mobile service providers are also selling your data on the black market. The upshot is that anyone with a mobile phone is vulnerable to being watched by stalkers, criminals, low-level enforcement officers who do not have a warrant, and other curious third parties who may
have very questionable intentions and no right to access our sensitive data. In the United States, obtaining real-time updates on any mobile phone’s location costs around $12.95.\textsuperscript{59} While this underground market for location data has only been confirmed in the United States with respect to T-Mobile, Sprint, and AT&T, it may well be happening with other telecoms and in other parts of the world.

Car companies, data brokers, telecoms, shops, and tech giants all want to know where you are. You might find it reassuring to think that, even if it’s true that huge amounts of data about you are being collected, much of it will be anonymized. Unfortunately, all too often it is easy to re-identify anonymized data. One of the first lessons in re-identification came from Latanya Sweeney in 1996, when the Massachusetts Group Insurance Commission published anonymized data showing the hospital visits of state employees. Then Governor William Weld assured the public that patients’ privacy was safe. Sweeney proved him wrong by finding his medical records in the data set and mailing them to his office. She later showed that 87 per cent of Americans could be identified with three pieces of data: birth date, gender, and zip code.\textsuperscript{57}

Another way in which you could be identified is through your location. Every person has a different location footprint, so even if your name is not on the database, it’s easy to work out who you are. The specificity of location data is not surprising, given that there is usually only one person who lives and works where you do. Yves-Alexandre de Montjoye, head of the Computational Privacy Group at Imperial College London, studied fifteen months of location data for 1.5 million individuals. De Montjoye and his colleagues found that, in a data set in which people’s locations are recorded on an hourly basis with a spatial resolution equal to that given by mobile phones as they connect to cell towers, it is enough to have four spatiotemporal data points to uniquely identify 95 per cent of individuals.\textsuperscript{58} Similarly, when researchers looked at three months of credit card records for over a million people, they found that they needed only four spatiotemporal data points to uniquely re-identify 90 per cent of individuals.\textsuperscript{59}

Databases can often be de-anonymized by matching them with publicly available information. In 2006, Netflix published 10 million movie rankings by half a million customers as part of a challenge for people to design a better recommendation algorithm. The data was supposed to be anonymous, but researchers at the University of Texas at Austin proved they could re-identify people by comparing rankings and timestamps with public information in the Internet Movie Database (IMDb). Movie preferences are sensitive; they can reveal political and sexual tendencies. A lesbian mother sued Netflix for putting her at risk of being outed.\textsuperscript{60}

Data brokers are misleading the public when they claim they anonymize data.\textsuperscript{61} They trade in personal data. They collect all kinds of extremely sensitive information, package it, and sell it to banks, insurers, retailers, telecoms, media companies, governments, and occasionally, criminals.\textsuperscript{62} These companies sell information about how much money you make, whether you are pregnant, or divorced, or trying to lose weight. They have also been known to sell lists of rape victims, AIDS patients, and other problematic categories.\textsuperscript{63}

Online ads also use questionable categories to target individuals. The Interactive Advertising Bureau, a trade group that establishes industry norms, uses categories for targeted ads that include incest or abuse support, substance abuse, and AIDS/HIV. Google’s categories to target people for ads likewise include substance abuse, sexually transmitted diseases, male impotence, and political leanings.\textsuperscript{64} These categories show what data vultures are interested in: they are eager to know where we hurt the most. Like
predators, they can smell blood. They look for our vulnerabilities in order to exploit them.

Let’s go back to your day. We left you packing for your work trip to the United States. When you get to Heathrow airport, you might not be asked for your boarding pass as you go through security and later board the plane. Facial recognition is now being used to verify your identity.66

When you arrive at your destination, a Transportation Security Administration (TSA) officer asks you to surrender your laptop and smartphone. You try to resist, but he informs you that if you deny his request, you will be refused entry. You have a work event to get to. If your boss learns that you did not attend that meeting because you were deported for disobeying an officer at border control, he will not be pleased, to put it mildly. You wonder whether he might even fire you. The thought of being unemployed motivates you to surrender your most private data. You try to think about the kind of data you have in there. You think about the nude photos with your spouse, photos of your children, all your financial information.

Then it occurs to you that you also have very private information regarding your employer. Perhaps you have business secrets that are worth millions. How can you be sure that data will not end up in the hands of an American competitor? Or perhaps you have confidential information about your government that you produced or acquired when you worked as a consultant. In 2017, a NASA engineer was forced to unlock his smartphone at the border, even though it had sensitive content on it.66 Or maybe you are a doctor who has sensitive information about your patients on your laptop, or a lawyer protecting your clients, or a journalist protecting your sources.

You tell the TSA officer that you have to protect whatever confidential information you have – it is your professional duty, and you could face legal consequences if you do not. The TSA officer is unmoved. You remember reading something in the press about how, if you get deported from a country, you have to stay away for five or ten years. That would be fatal for your job. You’re not sure whether ‘refused entry’ equals deportation. You ask for a lawyer. The TSA officer responds by saying that, if you want a lawyer, you must be a criminal. He asks whether you have something to hide. Weary and intimidated, you end up complying and handing over your laptop and phone. He takes your electronic devices away from your sight for a quarter of an hour or more. In that time, he downloads your data.67

Smart borders are becoming threats to civil liberties; they are being rolled out without seriously evaluating their benefits, risks, and legal and ethical implications.68 Drones, sensors, and facial recognition, among other invasive technologies, promise cheaper and more effective border control at the cost of our privacy. Given its failure (so far) to fund a brick wall at the border with Mexico, the Trump administration is building a virtual wall made of surveillance. Sensors are not only deployed at the actual border, but also in American communities close to the border.69 Similar initiatives are being proposed and tested around the world. Hungary, Latvia, and Greece are piloting an automated lie-detection test at four border points. The system, called iBorderCtrl, asks travellers questions such as ‘What’s in your suitcase?’ and then tries to identify ‘biomarkers of deceit’.70

You arrive at your hotel feeling exhausted, angry, and humiliated by the violation of your right to privacy. You resolve to do something to avoid or minimize future violations. You think about writing an email to an immigration lawyer, to be better informed about your rights. But you are afraid that the TSA, the
NSA (National Security Agency), or some other agency might get access to that message, and that might be enough to get flagged at airports. You don’t want to become that person who always gets stopped at borders and interrogated for hours at a time. You’re too afraid to ask for legal advice. Maybe it’s enough if you lessen the data your phone and laptop collect on you. It’s a start, in any case.

You might begin by trying to establish what data may have been downloaded from your phone and laptop. You download the data that Google and Facebook have on you. Horrific at the level of intrusion you discover (Google has data on you that you thought you had deleted), you decide you should change all your privacy settings to minimize data collection. When you look at your settings, you notice that all the defaults are set to undermine your privacy. And, while some of these settings can be changed, if you do not consent to some data collection, you cannot use the services provided by tech giants like Facebook and Google. There is no room for negotiating the terms and conditions, and these can change at any time without you being notified. You are being bullied.

It dawns on you that in many ways you are being treated as a criminal suspect. The level of intrusion, the geotracking as if you had an electronic bracelet attached to your ankle, and the forcefulness of it all. In some ways it’s worse than being a suspected criminal. At least when the police arrest you they allow you to remain silent, and warn you that anything you say may be used against you. As a subject of tech, you have no right to remain silent — trackers collect your data regardless of your not wanting them to — and you are not reminded that your data can and will be used against you. And at least during a trial you wouldn’t be forced to self-incriminate. In the surveillance society, your data is used against you all the time.

Your spouse interrupts your thoughts with a call. He is upset about the smashed Echo. Things haven’t been great between you for a while. You wish you had the serenity to tell him calmly what happened, but you feel defeated. Your silence causes an escalation in the distress your partner feels and expresses. ‘I’m sorry,’ he says, ‘I wish we were face to face, but I cannot stand a day longer in this situation. I would like a divorce. We’ll talk about the details when you come back.’ He hangs up on you.

Stunned, you open Spotify on your laptop to calm yourself down with music. The first ad that comes up is for a divorce lawyer. Is it a coincidence? Probably not. How did they know? And who are ‘they’? Maybe it was your spouse’s online searches for divorce. Or perhaps it was your marital fights that got recorded and analysed. Or maybe a predictive algorithm guessed your impending divorce based on how little time you have spent with your family lately. Maybe it was Spotify analysing your mood based on your music choice. Even bankers are gauging the public mood by looking at data from Spotify. It bothers you that you’ll probably never know who knows that you are getting a divorce, how they got that information, and whether they knew before you did. Whatever the case, it is not okay. You didn’t tell them, and they do not have a right to eavesdrop on your most intimate relationships.

You wonder how far the privacy invasions can go before we decide to limit them. Technology has always pushed the boundaries of privacy. First photography, now the internet. You shudder at the memory of the news that Nike has started to sell their first smart shoes. If researchers develop ‘smart dust’ — ubiquitous sensors that don’t need batteries and are tiny enough to be near invisible — privacy might become almost impossible to protect.

You are tempted to think that you’ll be glad to leave this brave new world behind, one day. You’re only sorry that your son has
had to cope with privacy problems from such a young age, and that he will have to deal with them for much longer than you. Pondering your mortality, it dawns on you that violations of your right to privacy will not stop with your death. You will keep on living online. Scavengers will keep living off the trail of data you leave behind. And perhaps that data may still affect your son and his offspring. It may also affect the way your life is perceived by others — your post-mortem reputation.

You wonder if there is anything you can do to clean up your data footprint before it’s too late. There is. Before yielding to despair over how we lose streams of privacy every second of every day, read on. The next three chapters do not paint a pretty picture, but taking a look at the grisly insides of the data economy is important to allow us to better understand how we got here, and how we can get out of this oppressive mess.

The contrast between today’s privacy landscape and that of the 1990s is stark. At the end of the twentieth century, your car was a car — it wasn’t interested in the music you like, it didn’t listen to your conversations, it didn’t track your weight, it didn’t record your comings and goings. Your car took you where you wanted to go. It served you. You didn’t serve it. For some of us, waking up to surveillance in the digital age felt as though we went to bed one night and found a completely different world the next morning — a bleaker one, at least with regard to our privacy and our autonomy over the objects surrounding us. How did we get here? Why did we allow the surveillance society to take root? At least three elements played a part in the erosion of our privacy: the discovery that personal data resulting from our digital lives could be very profitable, the terrorist attacks of 11 September 2001, and the mistaken belief that privacy was an outdated value.
NOTES

INTRODUCTION

1 Throughout the book I use ‘the data economy’, ‘the surveillance economy’, ‘surveillance capitalism’, and ‘the surveillance society’ almost interchangeably. We could, in theory, have a data economy that excludes personal data. We could trade in data that is about impersonal matters. But, at the time of writing, when people write about the ‘data economy’, they are often referring to the trade in personal data, so I use the ‘data economy’ as shorthand for the ‘personal data economy’.


3 Remember how, in the first Matrix film, Trinity and Morpheus had to get to Neo through the Matrix to get him out of there?

CHAPTER ONE

1 For more on self-tracking, see Gina Neff and Dawn Nafus, Self-Tracking (MIT Press, 2016).


4 Sam Biddle, ‘For Owners of Amazon’s Ring Security Cameras, Strangers May Have Been Watching Too’, Intercept, 10 January 2019.
Enhancing Technologies 1, 2018; Brian Merchant, 'How Email Open Tracking Quietly Took Over the Web', Wired, 11 December 2017.


28 When communications are end-to-end encrypted, companies can’t access their content, but Zoom could access video and audio from meetings, despite the desktop app stating that Zoom was using end-to-end encryption. Micah Lee and Yael Grauer, 'Zoom Meetings Aren’t End-To-End Encrypted, Despite Misleading Marketing', Intercept, 31 March 2020. A few months later, Zoom fixed some of its privacy problems, but it announced it was going to exclude free calls from end-to-end encryption. After experiencing a privacy backlash, it then promised end-to-end encryption to all users. Kari Paul, 'Zoom to Exclude Free Calls from End-to-End Encryption to Allow FBI Cooperation', Guardian, 4 June 2020. Kari Paul, 'Zoom Will Provide End-to-End Encryption to All Users After Privacy Backlash', Guardian, 17 June 2020.


32 Kashmir Hill, 'Facebook Recommended That This Psychiatrist’s Patients Friend Each Other', Splinter News, 29 August 2016.

33 Kashmir Hill, ‘“People You May Know”: A Controversial Facebook Feature’s 10-Year History’, Gizmodo, 8 August 2018.


35 Dan Tynan, 'Facebook Says 14m Accounts Had Personal Data Stolen in Recent Breach', Guardian, 13 October 2018.
36 Gabriel I. X. Dance, Michael LaForgia and Nicholas Confessore, ‘As
Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants’,
37 Kashmir Hill, ‘Facebook Was Fully Aware That Tracking Who People Call
and Text Is Creepy But Did It Anyway’, Gizmodo, 12 May 2018.
38 Natasha Singer, ‘Facebook’s Push For Facial Recognition Prompts Privacy
39 Alex Hern, ‘Facebook Faces Backlash Over Users’ Safety Phone Numbers’,
Guardian, 4 March 2019.
40 Zack Whittaker, ‘A Huge Database of Facebook Users’ Phone Numbers
41 For a list of Facebook privacy disasters from 2006 to 2018, see Natasha
Lomas, ‘A Brief History of Facebook’s Privacy Hostility Ahead of
Zuckerberg’s Testimony’, TechCrunch, 10 April 2018.
42 Len Sherman, ‘Zuckerberg’s Broken Promises Show Facebook Is Not Your
Friend’, Forbes, 23 May 2018. ‘Despite repeated promises to its billions of users
worldwide that they could control how their personal information is shared,
Facebook undermined consumers’ choices,’ said Federal Trade Commission
Chairman Joe Simons. FTC Press Release, ‘FTC imposes $5 billion penalty
and sweeping new privacy restrictions on Facebook’, 24 July 2019.
43 Allen St John, ‘How Facebook Tracks You, Even When You’re Not on
Facebook’, Consumer Reports, 11 April 2018.
44 Digital, Culture, Media and Sport Committee, ‘Disinformation and “Fake
News”: Final Report’ (House of Commons, 2019).
45 Brian Fung, ‘How Stores Use Your Phone’s WiFi to Track Your Shopping
46 Stephanie Clifford and Quentin Hardy, ‘Attention, Shoppers: Store Is
47 Chris Frey, ‘Revealed: How Facial Recognition Has Invaded Shops – and
48 Kashmir Hill and Aaron Krolik, ‘How Photos of Your Kids Are Policing
49 Yael Grauer, ‘What Are “Data Brokers,” and Why Are They Scooping Up
Information About You?’, Motherboard, 27 May 2018.
50 Adam Tanner, Our Bodies, Our Data. How Companies Make Billions Selling
Our Medical Records (Beacon Press, 2017), 78, 95, 147–148.
51 Julia Powles and Hal Hodson, ‘Google DeepMind and Healthcare in an Age
52 Dan Munro, ‘Data Breaches in Healthcare Total Over 112 Million
53 Alex Hern, ‘Hackers Publish Private Photos From Cosmetic Surgery Clinic’,

54 Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller and Aaron
Krolik, ‘Your Apps Know Where You Were Last Night, and They’re Not
55 Nick Satt, ‘How AT&T’s Plan to Become the New Facebook Could Be a
56 Joseph Cox, ‘I Gave a Bounty Hunter $300. Then He Located Our Phone’,
Motherboard, 8 January 2019.
57 Olivia Solon, ‘“Data Is a Fingerprint”: Why You Aren’t as Anonymous as
58 Y. A. de Montjoye, C. A. Hidalgo, M. Verleysen and V. D. Blondel, ‘Unique in
59 Y. A. de Montjoye, L. Radaelli, V. K. Singh and A. S. Pentland, ‘Identity and
privacy. Unique in the Shopping Mall: On the Reidentifiability of Credit
60 Ryan Singel, ‘Netflix Spilled Your Brokeback Mountain Secret, Lawsuit
61 Aliya Ram and Madhumita Murgia, ‘Data Brokers: Regulators Try To Rein
In The “Privacy Deathstars”,’ Financial Times, 8 January 2019.
62 Natasha Singer, ‘Data Broker Is Charged With Selling Consumers’
63 Melanie Hicken, ‘Data Brokers Selling Lists of Rape Victims, AIDS
64 Nitasha Tiku, ‘Privacy Groups Claim Online Ads Can Target Abuse
65 Nicole Kobie, ‘Heathrow’s Facial Recognition Tech Could Make Airports
More Bearable’, Wired, 18 October 2018; Gregory Wallace, ‘Instead of
the Boarding Pass, Bring Your Smile to the Airport’, CNN, 18 September
2018.
66 Kaveh Waddell, ‘A NASA Engineer Was Required To Unlock His Phone At
67 Daniel Victor, ‘What Are Your Rights if Border Agents Want to Search
68 Gemma Galdon Clavell, ‘Protect Rights at Automated Borders’, Nature
543, 2017.
69 Olivia Solon, ‘“Surveillance Society”: Has Technology at the US-Mexico
Border Gone Too Far?’, Guardian, 13 June 2018.
70 Douglas Heaven, ‘An AI Lie Detector Will Interrogate Travellers at Some
71 Dylan Curran, ‘Are You Ready? Here Is All The Data Facebook And Google
72 John Naughton, ‘More Choice on Privacy Just Means More Chances to Do
What’s Best for Big Tech’, Guardian, 8 July 2018.
CHAPTER TWO

4 Samuel Gibbs and Alex Hern, ‘Google at 20: How Two “Obnoxious” Students Changed the Internet’.
8 Steven Levy, In the Plex: How Google Thinkers, Works, and Shapes Our Lives, 82.
9 Samuel Gibbs and Alex Hern, ‘Google at 20: How Two “Obnoxious” Students Changed the Internet’.
13 Jennifer Lee, ‘Postcards From Planet Google’.
19 Shoshana Zuboff, The Age of Surveillance Capitalism, 89.
23 Bruce Schneier, Click Here to Kill Everybody. Security and Survival in a Hyper-Connected World (New York: W. W. Norton & Company, 2018), 65.
25 Edward Snowden, Permanent Record (Macmillan, 2019).
26 Edward Snowden, Permanent Record, 223–224.
27 Edward Snowden, Permanent Record, 278–279.
28 Edward Snowden, Permanent Record, 163.
29 Edward Snowden, Permanent Record, 225.
30 Edward Snowden, Permanent Record, 167–168.
34 ‘Report on the President’s Surveillance Program’ (2009), 637.
35 For more on why mass surveillance is not the right approach to preventing terrorism, see Bruce Schneier, Data and Goliath, 135–139.