
tanosec

A Guide to Data Privacy: What it means for you, Why you should care, and How to take back control.

Table of Contents

CH 01.

Introduction

Introduction

Chances are, you didn't open this looking to read about data privacy. You're checking WhatsApp. Maybe scrolling Facebook, or catching up on TikTok. That's not a guess. WhatsApp and Facebook are by far the most-used platforms in South Africa, and Facebook alone reaches a majority of the population every month.

That's not a criticism. It's the point. Every app fighting for your attention runs on the same quiet trade: the platform is free, and in exchange, you are mined for information. The more a platform knows about you, the more precisely it can sell your attention to advertisers — and increasingly, the more valuable you become to people with worse intentions than advertising.

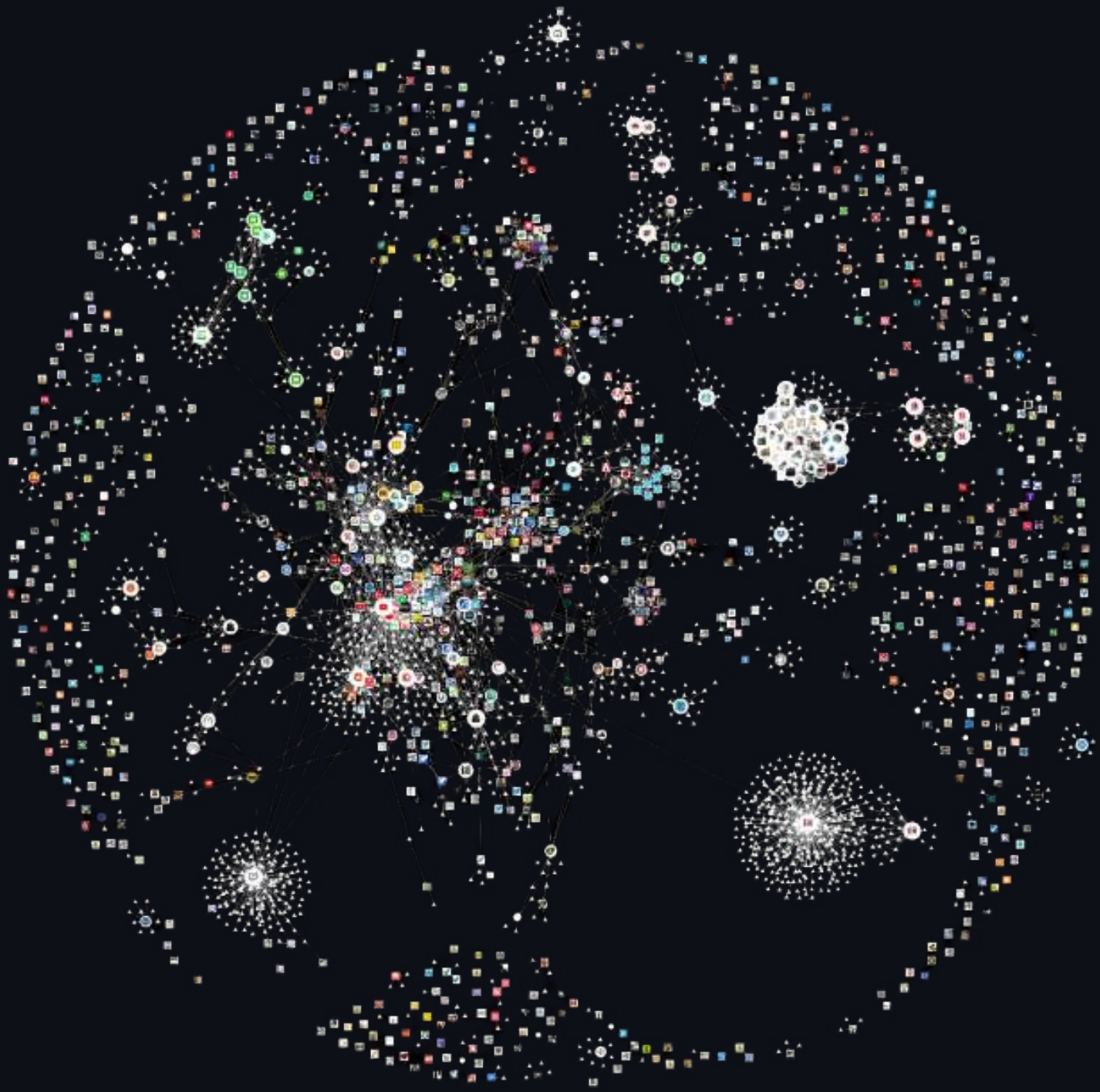
South Africa has felt this shift more directly than most. Digital banking fraud jumped sharply in the past year, and SIM-swap fraud alone now accounts for the majority of mobile banking fraud cases in the country — attacks that start with exactly the kind of personal data this guide is about. Your phone number, ID number, and banking details aren't abstract "data points." In South Africa right now, they're the raw material for a fraud economy that costs victims real money, often their life savings.

This isn't a call to delete every app and go off-grid. It's an invitation to understand the trade you're making — clearly enough to decide, on purpose, what's worth it and what isn't.

This guide is built in five parts:

- The What — what data privacy actually means, and what "personal data" covers
- The Why — why it matters, even if you feel you've "got nothing to hide"
- The How — how your data actually gets collected, often without you noticing
- The Who — who ends up holding it, and what South African law does (and doesn't) do about it
- Take Back Control — practical, tool-based steps you can act on today

This is only an introduction to a complex subject. Our hope is that by the end, you'll be equipped to make more deliberate choices about your data — and know where to go if you want to dig deeper.



Firefox Lightbeam is a browser extension that uses interactive visualizations to show you the relationships between third parties and the sites you visit

Over the course of 8 months, Lightbeam tracked 1,111 websites visited, and recorded 2,007 third party sites that those websites connected and shared data to.

Source: Reddit User Daniellynet

CH 02.

The What

So what is data privacy, anyway?

Data privacy is about how information should be handled based on how sensitive it is. You wouldn't think twice about telling a stranger your first name. You'd think very differently about handing over your banking PIN. That instinct — some information is fine to share, some isn't — is data privacy in a sentence.

The complication is scale. In a normal day, you might knowingly share your name a handful of times. Online, platforms are quietly collecting far more than that, far more often, about things you'd never think to guard: how long you paused on a photo, which ad you almost clicked, what time you usually go to bed based on when your phone stops moving.

Companies aren't collecting this out of curiosity. In a competitive market, more data means a sharper picture of you — and a sharper picture sells better, whether that's a product, an ad, or in some cases, a political message. Your platforms very likely know more about your habits, routines, and moods than your closest friends do. Most of us have never sat down and decided that was an acceptable trade — it just happened, one "Accept All Cookies" click at a time.

What do we mean by “Personal Data?”

“Personal data" is a broad umbrella. It's useful to break it into categories, because not all of it is treated — or protected — equally:

Identity Data

- Personal information: name, ID number, phone numbers, email addresses, social handles
- Demographics: age, gender, language, relationship status, education level
- Location: recent and planned locations, home and work addresses

Read: How Companies learn your secrets - The New York Times

Quantitative Data

- Transactional: purchases, subscriptions, returns, abandoned carts
- Communication: who you message, when, how often, on which platforms
- Online activity: sites visited, posts liked, accounts followed

Descriptive Data

- Life events: relationship changes, new jobs, moving house, having children
- Lifestyle: property owned, vehicle owned, pets, income bracket
- Interests: entertainment, shopping, and food preferences; travel habits.

Read: The Hidden World of Privacy Policies

Qualitative Data

- Attitudinal: reviews you leave, ratings you give
- Opinion: favourites, wishlists, things you've said you want
- Motivational: what actually drives your purchases — price, brand, urgency, gifting

In South Africa, a few categories carry particular weight. Your ID number is a master key — it links your identity, banking, telecoms, and government records in a way a name or email alone doesn't. Your phone number is functionally your bank account's second password, thanks to OTP-based banking security — which is exactly why SIM-swap fraud has become such a lucrative crime here. Data that feels harmless elsewhere can be the exact piece of information a South African-focused scam needs.

I've got nothing to hide.

All this data is collected under a wide, open-ended spectrum of consent: Sometimes the data is shared knowingly, and other times (more often that not), the users might not understand they're giving up anything at all. While sometimes it's clear that something is being collected, the specifics and minutia of it are often hidden and buried in hard-to-parse terms-of-service agreements, that, let's face it, no one actually ever reads. There are also cleverly designed Dark UX Patterns (more on this later), that make you want to click and do things that you never intended to do. In 2012, Target figured out how to determine whether a woman was pregnant or not, sending them a slew of personalized ads. Where this got especially creepy, however, was when the teenage daughter of a man in Minneapolis was sent coupons for baby clothes and cribs. While the father was enraged at why these coupons were being sent to his daughter, little did he know that she was, in fact, due later that August.

Let's look at another example, what happens when someone sends a vial of saliva to 23andme, Ancestry, Natera or FamilyTreeDNA? The person knows they're sharing their DNA with a genomics company, but they may not ever realize that their information will also be sold to pharmaceutical companies. Many apps also use your location information to show you custom adverts, but they don't necessarily advertise the fact that certain hedge funds may also buy that location data to analyze which stores you frequent. Any online shopper who's seen ads directly targeted towards their interests knows they're being tracked around the web, but fewer people understand that those companies may also be recording not just their clicks, but also their exact mouse movements.

In each of these scenarios, the user received something in return for allowing a corporate entity to monetize their personal data; They got to learn about their genetic ancestry (although, on average, a service like this costs upwards of $100), use a mobile app, or browse the latest footwear trends from the comfort of their homes.

This is the same sort of transaction you make with Facebook and Google. Their core products and services, including Instagram, Messenger, Gmail, and Google Maps, don't cost money. You pay with your personal data, which is used to target you not only with ads but with your ideologies as well.

CH 03.

The Why

I've got nothing to hide.

Your information has value. Companies like Facebook and Google allow you to upload unlimited data to their servers, for free. What's their business model? How do they make so much money? They sell your info to advertising companies and data brokers. But they never asked you if you wanted to sell your information. If someone asked you, in person, 100 questions about your personal life with the intent of selling the information, would you answer them? Probably not, right? But you let this happen every time you use a service that makes money selling your info.
Other than value, there are two sets of reasons to care about your privacy even if you've got nothing to hide—ideological reasons and practical reasons. Ideologically, privacy is a right that we haven't always had. Just like the right to freedom of speech, generations before ours have fought for our right to privacy as a human right.

Having nothing to hide is not true nor realistic. Don't confuse privacy with secrecy. Everyone knows what you do in the bathroom, yet you still close the door. That's because you want privacy, not secrecy. Just like you have a passcode for your phone, and passwords for your email because you don't want people reading your personal messages.

Practically, especially, information in the wrong hands becomes dangerous. You might be okay with governments or security agencies having your private information. You might even trust Google or Facebook with all of your information. But what if these trusted platforms get hacked and your information falls in the wrong hands? What, or who would your information make you vulnerable to? You also can't predict the future. Right now you may not have a lot to risk, but what about 30 or 40 years from now? If Sony's hacking has told us anything, it is that your private information has an impact on your life. Amy Pascal, co-chairman of the company, lost her job because of the company's reckless security.

Your private life out of context becomes a weapon. In “secure chats” or closed doors with friends or colleagues, we’ve all made comments or said things that we regret, or might be misinterpreted by others out of context. In fact, our behavior changes depending on the people we’re with. Someone could easily find something offensive you said in a group chat that you have with your closest friends. Because they’re your friends and it was a joke or a sarcastic remark. But take it out of context and it is no longer a joke.

With the 2020 COVID-19 pandemic forcing people to stay home, work from home, and now spend more time on their digital devices than ever before, it becomes imperative to talk about why privacy matters. As schools and businesses transitioned to conduct classes and meetings on the popular video conferencing app, Zoom, little did they know that their data was also being shared with Facebook, regardless of whether they were Facebook users or not. When caught publicly, Zoom quickly reversed the code to stop sharing data with Facebook. Yet another bug in the app’s code also made it possible for what is now referenced to as “Zoombombing”—trolls of the internet jumping into public Zoom calls and using the platform’s screen-sharing feature to project graphic content to unwitting conference participants, forcing hosts to shut down their events.

As we increasingly become more and more dependent on these technologies, we must ask ourselves about the tradeoffs we’re making by using these services. We must demand oversight change on an industry-wide level.

Read: How Zoom was selling data to Facebook. even if you weren’t a Facebook User

The South African Stakes

This isn't abstract in South Africa right now. A few things worth sitting with:

Your data is directly tied to fraud risk here. SIM-swap fraud — where a criminal convinces (or bribes) your mobile network into transferring your number to a SIM they control — remains one of the most damaging fraud categories hitting South African bank accounts, precisely because so much of our banking security runs on OTPs sent via SMS. The starting point for a SIM-swap attack is almost always personal data gathered elsewhere first: your ID number, phone number, and enough personal detail to convincingly impersonate you to a call centre agent.

AI has made impersonation cheaper. Voice-cloning and deepfake scams — where a "family member" or "boss" calls sounding exactly like themselves, asking for an urgent payment — have moved from novelty to a real and growing threat category, built entirely from publicly available audio and video of you or people you know. The more of your voice, face, and personal details that are public, the more raw material exists for this kind of fraud.

The law is catching up, but slowly, and mainly protects you after the fact. South Africa's Protection of Personal Information Act (POPIA) is the closest thing we have to comprehensive data protection law, enforced by the Information Regulator. It's worth knowing what it actually does: it obliges companies handling your data to do so lawfully, securely, and transparently, and gives the Regulator power to fine non-compliant organisations up to R10 million per violation. Enforcement has visibly picked up — the Regulator has issued its first R5-million fines and moved into proactive compliance monitoring of organisations rather than only responding to complaints.

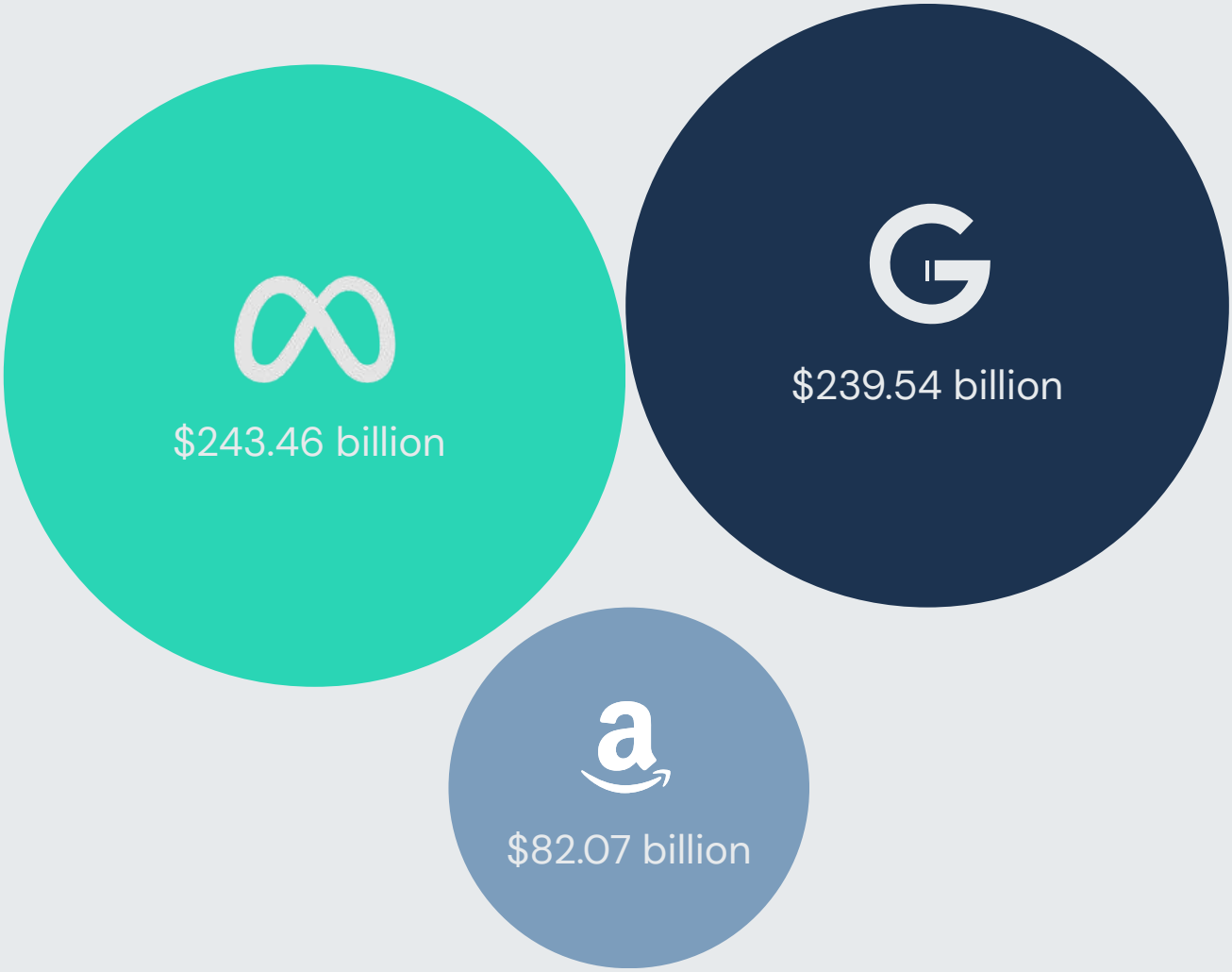
What POPIA doesn't do is stop your data from being collected in the first place. It governs how organisations must handle data once they have it — not whether they should have been allowed to collect it at all. That distinction matters: POPIA can punish a company after your data leaks in a breach. It won't stop a legitimate business from harvesting far more of your personal information than you'd knowingly agree to, provided they disclosed it somewhere in a privacy policy you never read.

Why this matters more now than it used to

Two shifts have made this decade different from the last:

- More of life runs through fewer platforms. Banking, communication, work, and social life increasingly funnel through the same handful of apps, meaning a single compromised account can cascade into several areas of your life at once.
- AI has lowered the cost of using your data against you. It used to take real effort to impersonate someone convincingly. Now it takes a few voice notes and a generative AI tool. The personal data you've shared over the years — casually, in good faith — is exactly the raw material this depends on.

None of this is a reason to panic. It's a reason to be deliberate. The rest of this guide is about understanding how your data actually moves, so the choices you make about it are informed ones.



Combined, these three platforms now account for 62.3% of all global digital ad spending. Global digital ad spend overall is approaching $800 billion in 2026

Source: EMARKETER, April 2026 forecast.

17.

Source: South African national privacy survey (Column Inc/AmaBhungane, reported via The Conversation)

CH 04.

The How

How your data actually gets collected

Humans have used devices to collect data about the world for many years now. Greek scientists used an intricate gear system called the Antikythera mechanism, to trace astrological patterns as far back as 150 BC. Two thousand years later, Herman Hollerith invented the tabulating machine, a device that helped process data from the 1890 United States Census. Hollerith founded the company that later merged to become what is now IBM.

Most people picture "data collection" as something that happens when you fill in a form. In reality, most of it happens silently, in the background, while you're doing something else entirely. Here's what's actually running under the hood of your everyday browsing and app use:

Cookies
Small pieces of code deposited in your browser that let sites remember you across visits. Some are genuinely useful (keeping you logged in, remembering your cart). Others exist purely to follow you from site to site, building a profile of everywhere you've been.

Fingerprinting
Instead of a cookie, this method identifies you by the unique combination of your device's characteristics — screen resolution, installed fonts, browser version, even battery level. You don't need to accept anything for this to work; your device's own uniqueness is the tracker.

App permissions
Every "Allow" tap on a permission prompt — location, contacts, microphone, camera — is a data tap being opened. Many apps request far more than they need for their core function. A flashlight app rarely needs your contact list.

Location pings
Apps with location access don't just check in occasionally — many request your GPS position hundreds of times a day, even when you're not actively using them, quietly building a detailed map of your daily movements.

Social logins
("Sign in with Google/Facebook") Convenient, but it means the platform you log into and the platform you logged in with both get a record of the interaction — often more information than either needed to complete the login.

Dark UX patterns
Some data isn't collected passively — it's collected because interfaces are deliberately designed to make you share it. Pre-ticked checkboxes, confusing double-negative wording ("uncheck this box if you don't want to not receive marketing"), and buried opt-outs all exploit the fact that most people skim rather than read closely. This isn't accidental complexity — it's a designed outcome.

Identity Trackers
Instead of using a cookie, these rare trackers follow people using personally identifiable information, such as their email address. They collect this data by hiding on login pages where people enter their credentials.

Session Cookies
Some trackers are good. These helpful same-site scripts keep you logged in to websites and remember what's in your shopping cart—often even if you close your browser window. However, these can be exploited by websites with ill intent.

Session replay Scripts
Some same-site scripts can be incredibly invasive. These record everything you do on a website, such as which products you clicked on and sometimes even the password you entered.

Social Media Trackers
Logging into websites using your Google or Facebook account can often be a handy and streamlined way of creating accounts, but you're also duped into sharing way more information that you need to, not just with that website, but also the platform you used to log in. This also applies to embedded posts, tweets, and youtube videos that you see in articles across the internet.

Email Trackers
For popular email services like Gmail and Yahoo, your emails are also scanned for keywords, interests, and topics you like—helping advertisers sell to you better. But that's not all, newsletters you receive are also ways in which you are tracked and profiled for the services and apps you use.

Keep in mind that this is just your web browser, using apps and other plugins can afford the platforms other backdoors to keep tabs on you. Here are a few ways in which using Apps and Plugins can allow for more avenues in tracking you:

Read: How the New York Times was able to track Donald Trump and members of the Secret Service through publically available GPS data

Watch: see how this unconventional game, winner of apples design award makes use of your phones sensors to create innovative puzzles

Location Data
This one is rather straight-forward: Apps can capture your GPS data and send them to their respective servers for storage and analysis. Google Maps, for example, sends upwards of 300 location pings daily on an Android phone.

Bluetooth Scanning Data
Apart from your location data, if you have your Bluetooth enabled at all times, your device will intermittently capture other Bluetooth devices available to connect to. These devices can share their names, device types, and other identifying information that can be used to fingerprint you further.

WiFi Scanning Data
Much like Bluetooth scanning, your phone and laptop will also scan for available public networks available to connect to. This information can contain the network name, location, IP addresses that can be used to pinpoint your location. So even if you have your location services disabled, ill-intent apps can still triangulate your estimated position through these scans.

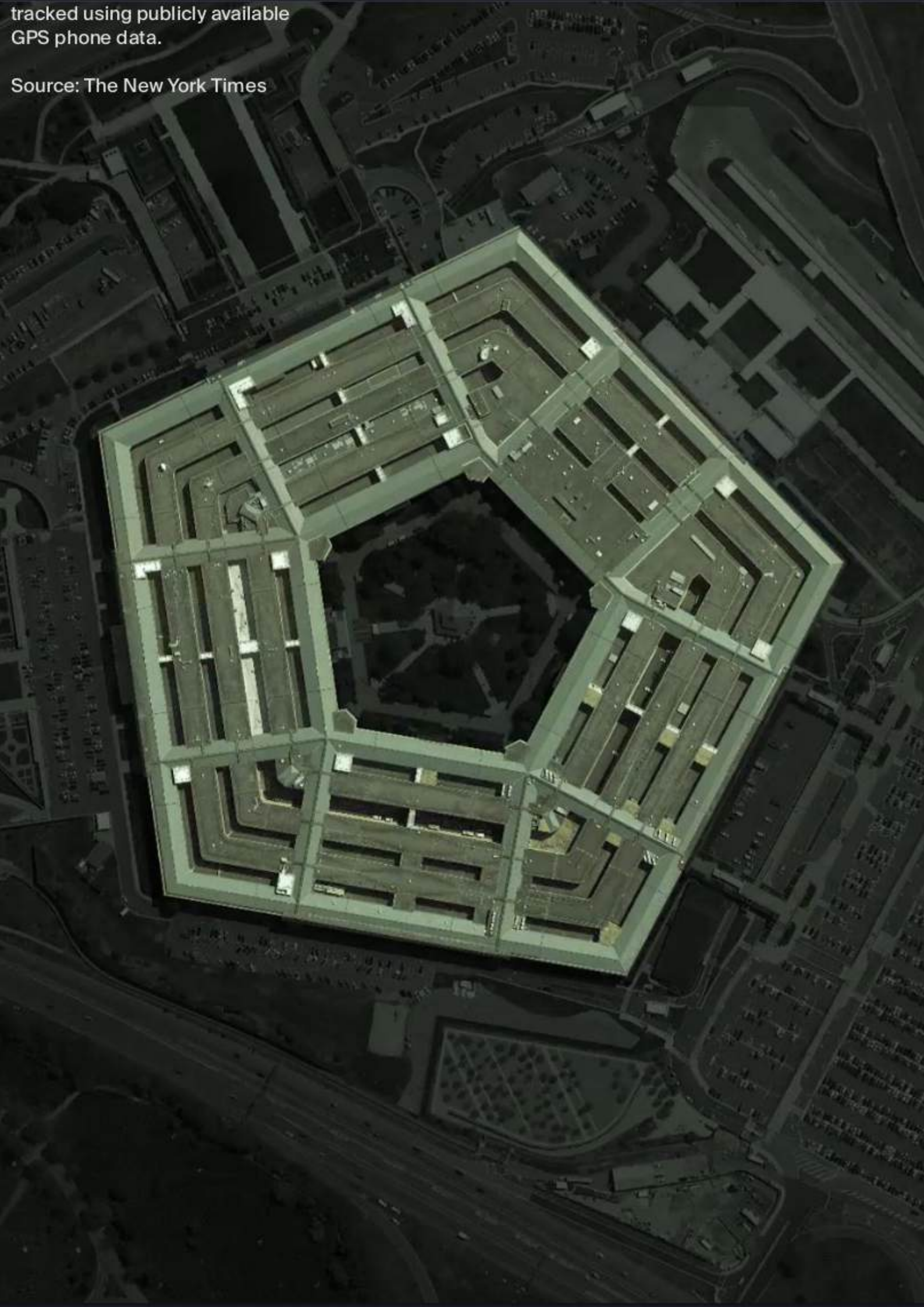
Read: More about Dark UX Patterns

Device Identifiers
Your device, by itself, can also reveal a lot about you: An app can request the name, make, model, serial number, network carrier information, and even the color of your phone, to create a unique fingerprint of you.

Device Sensor Data
Perhaps the scariest of the list is your device sensor information. Modern devices, like the iPhone 11 Pro, contain a vast array of advanced sensors that can detect your physical state (i.e. sitting, lying, walking), your location, your ambient lighting conditions, and ambient sound information. In some cases, apps were able to get personal health information from your device, which can include information like age, weight, height, and even heart rate data.

tracked using publicly available GPS phone data.

Source: The New York Times



The future of Data Collection

Data collection in our current technical landscape has primarily been done through screens when people use computers and smartphones. However, the coming years will bring new data-guzzling devices like wearable health tech, sensor-embedded clothing, AR glasses, smart lights, home automation tech, and so much more. We've already seen a glimpse of these products through products like smart speakers and the several scandals they've already been in. But even for those who refrain from using these devices, will likely have their data gathered, with the adoption of facial recognition-enabled cameras across the most urbanized cities. In so many ways, this future has already begun—Taylor Swift fans have had their faces collected, and Amazon Echoes and Google Homes around the world have been listening in on millions of homes.

Watch: Netflix's Black Mirror - S01E03: The Entire History Of You

We haven't yet decided, though, how should we navigate this new data-harvesting landscape. Afterall, we can't expect laws from nearly 50 years ago to keep up with the rapidly changing landscape of the tech industry. Do we really want health insurance companies tracking our eating and shopping habits? Should colleges be permitted to digitally track their applicants through their social media? It is now more imperative than ever, to start asking these questions.

Watch: Her (2013), directed by Spike Jonze, starring Joaquin Phoenix and Scarlett Johansson

Perhaps, as scientists continue to push the boundaries of what's possible with artificial intelligence, we will also need to learn to make sense of the personal data that isn't even real, but fabricated by algorithms that other machine learning algorithms can train on. With the rise of the so-called deepfake technologies, propagandists and hoaxers can now leverage social media photos to recreate videos that depict events that never happened.

AI can now create millions of synthetic faces that don't belong to anyone, altering the definition of identity-theft. This fraudulent data could further blur the line between what's real and what's fake on social media. Imagine trying to discern whether your Tinder match or the person you just followed on Instagram is actually real or not.

Regardless of whether data is fabricated by computers or created by real people, a big concern yet remains on how this data will be analyzed. It's important to understand that not only the information we collect matters, but what inferences and predictions we make from that data that matters equally, if not more.

Our personal data is already being used by algorithms to make important decisions like whether someone should maintain their health care benefits, or if someone should be released on bail. These decisions can easily be biased, and researchers at companies like Google are now working on making algorithms and the datasets that are used to train them, more transparent and fair.

Tech companies are now also beginning to acknowledge that data collection needs to be regulated. While Microsoft has called for the federal regulation of facial recognition technology, Apple's CEO Tim Cook has called on the FTC to establish a clearinghouse where all data brokers will need to register. Some companies and researchers argue, however, that it's never going to be enough for the government to simply protect personal data; Consumers will need to take ownership of their own data, and be compensated for when it's used. Social media like Minds and Steemit, as well as the privacy focussed browser, Brave, have already experimented with rewarding users with cryptocurrency in exchange for some pre-vetted ads. Other companies will pay you in exchange for sharing your data, for example, the app Sweatcoin tracks your steps, and offers free products through spending the accumulated in-app currency. There are, however, doubts about people taking ownership back as well, as it won't solve every privacy issue posed by the collection of personal data. Instead, it might be more practical to reframe the problem—perhaps less collection should be permitted in the first place and businesses should be encouraged to move away from the targeted-advertising business model altogether.

Read: Influencer Mia Zelu has racked up over 167k online followers despite not even being real

Photo: Instagram.

Photo: Instagram.

Can data collection help train Artificial Intelligence to cure lonliness and help us find true love? If so, would we want to?

Source: *Her (2013)*

CH 05.

The Who

The industry you never signed up for

Beyond the platforms you actually use, there's an entire industry built on collecting, compiling, and selling personal information you never directly handed over: data brokers. They pull from public records (property, court, marriage records), purchased retail data, and information bought from other companies, then package it and sell it on — to marketers, insurers, and sometimes to far less scrupulous buyers.

This information doesn't need to be accurate to be valuable, and doesn't need your involvement to exist. You can never have used a single data broker's product, and still be thoroughly profiled by one.

What POPIA actually gives you

South Africa's Protection of Personal Information Act gives you real, specific rights over your data — not just vague protections:

- The right to know what personal information an organisation holds about you and why
- The right to access a copy of your data on request
- The right to correct or delete inaccurate or unlawfully held data
- The right to object to your data being processed for direct marketing
- The right to complain to the Information Regulator if an organisation mishandles your data

The Information Regulator is South Africa's enforcement body for these rights — the equivalent role the FTC plays in the US, or the ICO in the UK. It has real teeth: administrative fines of up to R10 million per violation, and it's moved from a mostly educational role into active enforcement, issuing its first R5-million fines and proactively auditing organisations' compliance rather than only responding to complaints.

Visit: Information Regulator (South Africa)

What POPIA doesn't cover

It's worth being clear-eyed about the limits:

- POPIA regulates how your data is handled once collected — it doesn't prevent a company from collecting large amounts of data in the first place, provided they disclose it (however buried that disclosure is)

- It applies to South African data — data brokers and platforms based entirely offshore, with no South African footprint, are harder to hold accountable

- Enforcement, while accelerating, is still catching up to the scale of the problem — most South Africans (63%, based on the survey in Chapter 3) don't even know where they'd report a violation.

The bottom line
Knowing your rights matters — but rights you don't know how to exercise don't protect you day-to-day. That's what the next chapter is for.

Mark Zuckerberg speaks to press and advertising partners in 2007. Two weeks after announcing its new marketing program, the company faced complaints from users surprised to find information about their online purchases added to their personal news feeds.

CH 06.

Take Back Control

Take Back Control

The bright side of all this is, the information you share online also contributes to the global store of useful knowledge—researchers from a number of academic disciplines study social media and other user-generated data to learn more about how we as a humanity functions. Author Seth Stephens-Davidowitz, in his book, Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are, argues that people are often more honest with sites like Google than they are in real life and traditional surveys. For example, he claims, fewer than 20% of people admit that they watch porn, yet there are more Google searches for “porn” than “weather”.

Read: Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us about Who We Really Are

Our personal data is also used by artificial intelligence researchers to train their automated models. Everyday, users around the world upload billions of photos, videos, gifs, texts, and audio clips to social media websites. This media is then fed to machine learning algorithms, so that they can learn to “see” and discern different parts of a photograph. Remember those annoying CAPTCHAs (Completely Automated Public Turing Test to tell Computers and Humans Apart) around the internet? The ones that ask you to prove that you are human? Yup, you guessed it, it’s actually using you to make itself smarter. So the next time you upload a selfie, you might actually make an AI smarter.

Understanding the problem is only useful if it leads somewhere. This chapter is deliberately tool-based, not lifestyle-based — because swapping out a setting takes five minutes; changing a habit takes months. Start here.

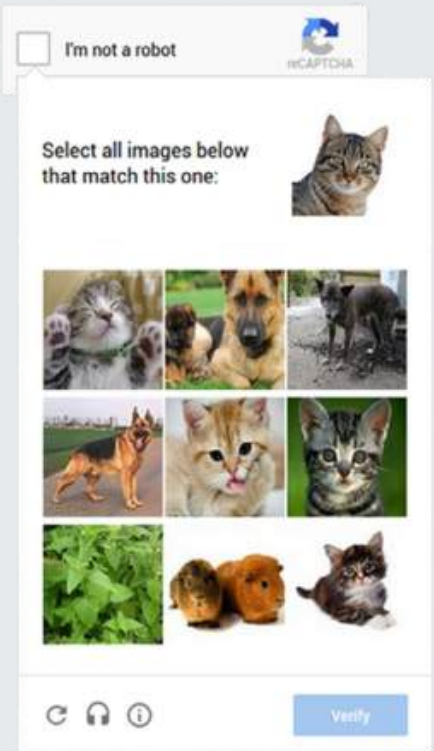


Photo: Google

15-Minute Wins

- Turn on two-factor authentication (2FA) on your email, banking, and social accounts — preferably using an authenticator app (Google Authenticator, Authy) rather than SMS, since SMS-based 2FA is exactly what SIM-swap fraud targets

- Review app permissions on your phone (Settings → Privacy) and revoke location, microphone, and contacts access for any app that doesn't genuinely need it

- Turn off ad personalization in your Google and Facebook account settings — this doesn't stop ads, but it stops them being built from your personal profile

- Check Have I Been Pwned (haveibeenpwned.com) to see if your email has appeared in a known data breach

- Delete unused apps and accounts — an account you don't use is still a place your data lives and can leak from

Visit:
haveibeenpwned

Weekend Project (30–60 minutes)

- Get a password manager (Proton Pass is Free) and stop reusing passwords across sites — a single reused password is often the first domino in a breach

- Review your social media privacy settings — audience for old posts, who can see your friends list, whether your profile is searchable by phone number

- Set up a "SIM-swap PIN" with your mobile network if they offer one — an extra verification step specifically designed to block SIM-swap fraud

- Register a request under POPIA with any company you're concerned about, asking what data they hold on you — you're legally entitled to this

For Business Owners

If you handle customer or staff data (and if you run a business, you almost certainly do), your obligations go further than personal hygiene:

- Confirm you have a registered Information Officer with the Information Regulator (this is one of the most commonly missed POPIA obligations for SMEs)

- Know what you'd do in the first 24 hours of a data breach — POPIA has mandatory breach reporting requirements

- Review what third-party tools (CRM, email marketing, analytics) have access to your customer data, and whether that access is actually necessary

This is the exact starting point of the security awareness and compliance work we do at Tanosec — if you'd rather have this audited and handled than DIY it, that's a conversation we're always happy to have.

CH 07.

Resources + About Tanosec

Further Reading

- Information Regulator of South Africa — inforegulator.org.za — file complaints, register as an Information Officer, read POPIA guidance directly from the source

- SAFPS (South African Fraud Prevention Service) — safps.org.za — protect yourself against identity theft and fraud specifically in the SA context

Visit: Electronic Frontier Foundation

Privacy & digital rights organisations

- Electronic Frontier Foundation (EFF) — eff.org — the leading nonprofit defending digital privacy and civil liberties; their Surveillance Self-Defense guide (ssd.eff.org) is one of the best plain-English resources on protecting yourself online

- Privacy International — privacyinternational.org — UK-based, strong global and policy-level coverage of surveillance and data exploitation

- noyb (None of Your Business) — noyb.eu — European privacy advocacy group, active in bringing real enforcement cases against major platforms

- Tech, Tactical. “The Data Detox Kit: Learn the Essentials.” Data Detox Kit, https://datadetoxkit.org/en/home.

Tools we'd point you to

Visit: proton.me

- Proton (Mail, VPN, Drive, Pass) — proton.me — privacy-focused email, VPN, and password manager, built on end-to-end encryption. We use Proton ourselves at Tanosec — it's a genuine recommendation, not a placeholder.

- Have I Been Pwned — haveibeenpwned.com — check if your email or phone has appeared in a known data breach

- Ethical Alternatives & Resources - https://ethical.net/resources/

A Closing Note

This guide only scratches the surface of a genuinely complex, fast-moving subject. Data privacy isn't a problem you solve once — it's a habit you maintain, the same way you'd maintain a lock on your front door. The goal was never to make you anxious about every app on your phone. It was to make the trade-offs visible enough that you're making choices on purpose, not by accident.

About Tanosec

Tanosec is a Bloemfontein-based offensive security consultancy. We test systems the way an attacker would, then translate what we find into plain-English findings and a clear plan to fix what's exposed — no jargon, no fear tactics. We work with South African SMEs on penetration testing, vulnerability assessments, phishing simulations, security awareness training, and POPIA-aligned security practices.

As featured in Sunday Times Ignite (April 2026), and a 2025 TechBehemoths Award winner for Cybersecurity Services in South Africa.

If reading this guide raised more questions about your own business's exposure than it answered, that's a conversation worth having.

Offensive Security for Defensive Results.
tanosec.co.za

Visit Tanosec's website

https://tanosec.co.za