The Smaller Kingdom

Leave less of your life lying about

Every record you leave is a bet on the future: on who will hold it, and on what the rules will be when they do. It is a bet you place without being told the odds, and you cannot take it back.

The usual argument about privacy happens in the present tense. Who can see this. What will they do with it. Whether you trust them.

That framing lets almost everyone off the hook, including you. Of course you trust them. They seem fine. You have nothing to hide.

But "nothing to hide" contains a hidden assumption: that what counts as something to hide has already been settled. It has not. It gets decided later, by whoever has power over you then, under rules nobody has written yet, in a country whose politics you cannot forecast, held by a company that may not exist in its current form by the time it matters.

Your data is patient. It will wait for those conditions to change. And it is very good at waiting.

Three things drift, and you control none of them

The holder drifts. Fifteen million people gave their genome to one company under one privacy policy. In March 2025 that company filed for bankruptcy and the genetic data became an asset in the estate. A court held that transferring it did not require anyone's fresh consent. What you agreed to was a policy, not a party. The full story is here.

The rules drift. People uploaded their DNA to a genealogy site to find cousins. Then it was used to catch a serial killer, and the terms were rewritten to allow that. Then an exception was granted outside those terms. Then the site made police searching opt-in, and the pool collapsed overnight. Then a detective obtained a warrant for the whole database, including everyone who had opted out, and it was handed over inside a day. Every one of those changes was made by somebody else.

Anonymity drifts. "Anonymised" is a claim about today's technique, not a property of the data. Search logs released as anonymous in 2006 had a named woman in Georgia identified from them within five days. Ratings released as anonymous were re-identified against a public film site. A researcher demonstrated that most Americans are uniquely identified by three ordinary facts. That history is here.

None of these were breaches. Nothing was stolen. Every one happened through the front door, legally, to data that had been given up willingly, by people who had nothing to hide at the time they gave it.

Why the total is a different thing

The mistake is in how we experience it. Data leaves us one piece at a time: a form, a cookie banner, an app permission, a post written in ten seconds about a politician. Each piece is small. Each is reasonable. Each is genuinely not worth the argument it would take to refuse.

But the thing that exists at the end is not a series of small pieces. It is a composite, and the composite has a property that none of its parts had.

It cannot be denied.

A claim can be disputed. If somebody says you are unreliable, you can produce a record showing otherwise. A profile cannot be disputed, because a profile makes no claim. It does not accuse you of anything. It simply sits there, every element of it accurate, every entry something you really did, and somebody else does the interpreting.

That is the trap, and it is why the usual advice misses. There is nothing in it to correct, because nothing in it is wrong.

And the reading is not fixed. The same record is a segment to a marketer, a risk to an insurer, and a disposition to a border officer, and it is read differently by each of them in each decade. This is worth sitting with, because it inverts the usual intuition: a fingerprint is a pointer, which identifies you and says nothing whatever about you, and can only be matched. A record of what you have said and bought and visited is content, and content can be read. In that one specific respect, the boring data is worse than the biometric. Nobody reinterprets a fingerprint. Everybody reinterprets a life.

The legal scholar Paul Ohm called the end state of this our personal "databases of ruin": the point at which enough separate records have been linked that there exists, for each of us, a record containing at least one fact whose exposure would do real damage. That argument is here. What is worth adding is that the damage does not require a secret. Your public life, assembled, is quite enough.

The right to delete arrives too late

An obvious objection at this point: if the conditions change, delete it. Europe even guarantees you that. Article 17 of the GDPR is titled the right to erasure, and it is real.

Now look at what happens when people use it.

When 23andMe filed for bankruptcy, about 1.9 million of its roughly 15 million customers requested deletion. The other thirteen million were not careless. They had used the thing once, years earlier, and nobody follows the bankruptcy filings of a company they have forgotten. At GEDmatch, people did exercise the right, in enormous numbers: the searchable pool fell from 1.2 million profiles to zero. Then a detective obtained a warrant covering the entire database, including everyone who had opted out, and it was handed over inside a day. AOL withdrew its released search logs within three days, by which time they had been mirrored beyond recall. And in this city, in 1943, people attempted to delete a database with fire, at the cost of twelve lives, and destroyed roughly fifteen per cent of it.

The pattern is a timing problem, and it is the quiet centre of this whole argument. **Deletion is a peacetime action.** You can only safely remove yourself from a database while it is still safe to be in it. By the time the record has become dangerous, the conditions that made it dangerous are usually the same conditions that make leaving impossible: the holder has changed hands, the copies have spread, a court has taken the decision away from everybody, or the government has.

The right to erasure is real, and it is available exactly when you do not need it.

Records outlive the reasons for them

The clearest illustration is not modern, and it is not comfortable, and it happened in this city.

From 1850 the Netherlands kept a continuous register of every resident, recording, among about twenty details, each person's religious denomination. It was built for municipal administration and social research, and in 1938 the man in charge of it described the coming system with evident pride as one that would follow each person "from cradle to grave".

Within three years, and under a different government, that same apparatus was used to register Jews and Roma.

We have written this up carefully, with the caveats historians insist on, on its own page. It is the origin of the phrase we keep coming back to: the register was not evil when it was built. It was just thorough.

So: a smaller kingdom

Not hiding. Hiding is exhausting, and it implies guilt you do not owe anyone. The move is duller and more durable than that: **reduce the surface**.

European law already contains this idea, aimed at the people who collect. Article 5 of the GDPR requires that data be "adequate, relevant and limited to what is necessary" for the purpose. It is called data minimisation, and it is a fine principle that you cannot enforce, because you are not the one holding the database.

The smaller kingdom is that same principle turned around and pointed at your own life. Fewer accounts. Fewer things that sync. Fewer conveniences that quietly file a copy somewhere you will never look. Not because any single one of them is sinister, but because the total is what gets sold, subpoenaed, breached, or read under rules that have not been written yet.

A record that was never made cannot be sold in a bankruptcy. It cannot be handed over on a warrant, or re-identified by a technique invented next year, or reinterpreted by a government you did not vote for. It is the only category of data with no future risk attached, and the only one you fully control.

The honest limits

A smaller kingdom is not invisibility, and anyone who sells you that is selling something.

Your bank has records. Your government has records, and mostly should. Your employer, your doctor, your phone company. Most of that is necessary, some of it is the price of living in a functioning society, and none of it is what this argument is about.

This is about the discretionary surface: the part you hand over casually, in exchange for a small convenience, because a well-designed screen asked politely and there was no obvious reason to say no.

We would also rather be accurate than frightening. Plenty of privacy warnings circulate that have no documented case behind them, and repeating them costs you the right to be believed about the ones that do. Where we make a claim, we cite it, and where the evidence runs out we say so on the page.

What we make

This is the belief underneath the workshop, so it is fair to say where it lands.

Every tool we sell is a single HTML file that makes no network calls. There is no account, no server, and no telemetry, which means there is no record of your use anywhere but in your own hands. That is not a policy we could change later, or a promise you have to take on trust. It is a property of the thing. We could not hand over your data under subpoena, or lose it in a breach, or sell it in a bankruptcy, because we do not have it. Read the philosophy if you want the longer version.

Elsewhere, at a studio called Meanwhile, we make Elba: an encrypted vault that is also one HTML file, with the same arrangement and the same consequence. Nothing to subpoena, nothing to breach, nothing hosted.

Neither of those is a solution to anything as large as the problem on this page. They are just two objects built as though the problem were real.

Read further

- Consent does not travel: what happens to your data when the company that holds it is sold, or dies.
- Anonymous does not stay anonymous: four decades of anonymised data being un-anonymised.
- Records outlive regimes: the Amsterdam population register, and what was done with it.

Frequently asked

What is data minimisation?

The principle that only the data actually necessary for a purpose should be collected and kept. It appears in Article 5(1)(c) of the GDPR, which requires personal data to be adequate, relevant and limited to what is necessary. The smaller kingdom applies the same idea to your own life rather than to the organisations collecting from you.

Why is 'I have nothing to hide' a weak argument?

Because it assumes that what counts as something to hide is already settled. It is decided later, by whoever holds power at that point, under rules that may not exist yet. Data collected today is read under tomorrow's conditions, and you do not get a say in what those are.

What happens to my data if a company goes bankrupt?

It is generally treated as an asset of the estate and can be transferred with the business. When 23andMe entered Chapter 11 in 2025, the court held that transferring customer genetic data to the buyer did not require fresh opt-in consent, because customers had been on notice through the privacy policy that data could be shared with corporate affiliates.

Is anonymised data safe?

Not reliably. Anonymisation describes the technique used at the time of release, not a permanent property of the data. Search logs, film ratings and census-style demographics have all been re-identified after being released as anonymous.

Does Offline.Ltd collect any data?

No. Every tool is a single HTML file that makes no network calls, so there is no account, no server and no telemetry. We could not disclose, lose or sell your data because we never receive it.

From Offline.Ltd, Amsterdam. The web version of this page lives at https://offline.ltd/smaller-kingdom and is kept current there.