Reflection · June 29, 2026

← Previous

You Are Not Anonymous

The trust you didn't choose

In plain English: with your email, anyone can find out in seconds where you have an account, and sometimes your face and name. This is not a bug: it is the internet working as usual. The question is not whether they can see you—they can—but who you are forced to trust. And there is only one place with nobody in the middle: talking directly, from one device to another.

An email address is enough. Not necessarily yours: any email. It is typed into a handful of free tools—legal, public, accessible to anyone who wants to search—and within seconds a list appears: which services that email is registered on, sometimes a profile picture, sometimes a first and last name that its owner thought they hadn't given to anyone. You don't need to be technical. No password is cracked. No crime is committed. All that information was already there—published, registered, or leaked—waiting for someone to take the trouble to put it together.

It is tempting to read this as a flaw: a breach, an oversight, something that someone should fix. It is not. This is the normal functioning of the open web. Every time you sign up for a service, fill out a form, post a review, or appear in someone else's leak, you leave a footprint. None of those footprints is serious on its own. The problem —if it is a problem—arises from connecting them, and connecting them is simple.

At this point, many people defend themselves with a reasonable phrase: 'I have nothing to hide,' or 'I take care of my accounts.' The former confuses hiding with choosing; we will return to that. The latter overlooks that you didn't leave most of that trail: it was left by the corporate registry, the website that suffered the leak, the acquaintance who uploaded a photo with you and tagged you. Anonymity on the internet is almost never a property you possess; it is, at most, obscurity: the provisional fact that no one has bothered to look yet.

So far we have talked about what a single person can do in a few seconds, by hand. Now remove the person. What has protected almost all of us for years was not anonymity, but disinterest: to find you, someone has to bother looking, and no one has the time to look at everyone. That last barrier—the effort of looking—is exactly what a machine lacks. An automated system can make that same cross-reference not against a target, but against an entire population; not once, but relentlessly; not out of suspicion, but by default. What used to take an investigator hours per person is now done on millions at once, without costing anyone time or attention. There is no need to guess who would want to do it—a company, a group, a State—; it is enough to understand that you no longer have to choose who to look at. You can look at everyone.

That is why 'can they find me?' is the wrong question. The answer is yes, and it will be increasingly so. The useful question is different: who, and how much, am I forced to trust in order to live connected? Because that is what you really do every day, almost always without thinking about it. You trust that the service where you register will keep your data safe. You trust that your carrier will not listen to your calls. You trust that the messaging app everyone uses—say, WhatsApp—does what it says it does. You trust the server in between, the company that manages it, the country where it is located, the free tool someone posted on the net. Each of those links is a trust decision. The difference is that you made almost none of them consciously: they came included. Those links that sneak in between you and the other person are called, in jargon, trusted intermediaries; the name matters less than the idea that they are there, and that there are many of them.

There is an honest way to verify all this: do it to yourself. And you don't need us to give you anything. Open your browser, type three or four words—something like 'what does the internet know about my email'—and the web itself will put the tools right in front of you. That ease is, on its own, half the answer: if you can find them in ten seconds, anyone can find what they say about you.

We do not offer you a list of our own, and that is deliberate. If we gave it to you, you would have to trust us: that we chose well, that those pages will still be trustworthy in five years, that behind none of them is—today or tomorrow—someone with bad intentions. We cannot promise that about pages we do not control, and we prefer not to make a promise we cannot keep. That is exactly what this article is about. But searching for it yourself comes with a price: the search engine does not distinguish the legitimate from the trap. Setting up a page that mimics a real tool, asks for your email, and keeps it is trivial. So, before typing anything anywhere, it's worth knowing how to read an address.

Note — reading an address before trusting it. A fake page can copy a real one down to the last pixel; what it can almost never forge is its address. Before typing anything on a site, read the address bar, not the page. The name that rules is the one glued to the left of the last part (`.com`, `.org`, `.co.uk`): in `secure-bank.weird-site.top`, the real owner is not your bank, it is `weird-site.top`. Distrust changed letters (a `0` for an `o`), extra words, hyphens where you don't expect them, and strange endings. The padlock and the `https` only mean that the connection is encrypted—not that the owner is honest—: a scammer also has a padlock. And the first results marked as 'ad' or 'sponsored' are there because someone paid, not because they are trustworthy. Each of those checks is, deep down, the same question: how much do I trust this address, and why?

At this point, it is worth describing the opposite of all this: a channel without intermediaries. Two people, alone on top of a mountain, talking. There is no postman, no switchboard, no server, no company, no country in the middle. And yet, notice: trust does not disappear there either. If you tell a secret to the other person, you are trusting them. That trust cannot be removed—nor does it need to be—because it is the only one you truly chose: you know who you trust, and why.

What isn't on the mountain is everything else. Nobody in the middle. And that, and no other, is the only model that can be honestly reproduced digitally: a direct channel from one device to another, with nothing and nobody along the way. It does not eliminate trust—that would be a lie—; it eliminates the intermediaries. It leaves you alone with the only unavoidable trust, the one you actually chose. That is, incidentally, the architecture from which we build these pages; but the argument stands on its own, whoever builds it.

So no, you are not anonymous, and you probably never will be again. But that was never the battle that mattered. You cannot live—nor browse—without trusting anyone; whoever tries is not freer, just more alone. Maturity is not distrust, which is just another form of naivety. It is being demanding: knowing who you grant your trust to, how much, in exchange for what, and—above all—knowing when you are granting it to someone without having decided to.

Almost nothing in life is black or white; almost everything lives in the gray in between, and learning to navigate that gray is a large part of what it means to have good judgment. The only exception is what comes well-made from the factory: that which, by design, asks you to trust no one other than the person you already decided to talk to. The rest—absolutely everything else—is a question of how much, and to whom.

Editor's note: when these Cuadernos name companies or products, it is not to accuse. Those who build them do work that millions of people use and appreciate. What we point out is structural — the model, not the brand. Brands appear as examples because they are the ones the reader recognizes.

Sources and further reading

- OSINT (open-source intelligence) — gathering information from already public data; it is neither intrusion nor espionage.
- Reglamento (UE) 2016/679 (RGPD) — on the processing of personal data, including the aggregation of data that was individually public.

- Public registries (corporate, judicial, property) — a legitimate and abundant source of personal information across most of Europe.
- In this same collection: the Cuadernos Lacre on end-to-end encryption and 'What a signature cannot fix' develop, from another angle, the same idea.

← PreviousWhat a signature cannot fix

Recent readings

- Reflection · May 27, 2026 What a signature cannot fix
- Analysis · May 26, 2026 Real vs. apparent privacy: the questions to ask yourself
- Analysis · May 25, 2026 Self-hosting as a professional practice

Take this article wherever you need it.

↓ Markdown ↓ Plain text ↓ PDF

The file is downloaded to your device. From there, you can save it, import it into Solo2, or share it as you wish. Cuadernos does not decide the destination for you.

Wax seal · SHA-256 12358f5f1b76fb344146dad35c9f70c558eb6c391cfc335ec3b264153d1412c3

Cuadernos Lacre · A publication of Menzuri Gestión S.L. ·
written by R.Eugenio · edited by the team of Solo2.