Analysis · May 16, 2026

← Previous·Next →

Encryption Is Not Privacy: What Metadata Tells About You

Encrypted content and visible metadata are two different things. When a service says "end-to-end encryption," it tells only half the story.

The Padlock That Doesn't Protect Everything

Most current messaging services advertise end-to-end encryption. And it is true: message content travels encrypted, so that no one along the way—not even the service provider—can read the text while it is in transit. To that extent, the statement is accurate.

The problem is that content is only part of the story. Even if no one can read what you say, the service does know other things with extremely high precision: who you talk to, at what time, with what frequency, from what approximate location, on what device, how many messages you send and receive, what number of files you share. All this is called metadata. And metadata tells, in many cases, almost as much as the message itself.

What Metadata Reveals

One does not need to read a message to know many things. If a person calls or writes to an oncologist every Tuesday at nine in the morning for six months, it is not necessary to listen to the conversation to guess what is happening. If two people exchange a hundred messages a day and suddenly stop, there is no need to read any of them to understand what has happened. If a tax advisor receives twenty consecutive messages from the same client the night before a quarterly close, the pattern speaks for itself.

Metadata reveals behavioral patterns: who interacts with whom, what schedules each person has, when they are awake, when they sleep, when they travel, which clients are most active, which professional relationships are most intense. A server that collects metadata can build a detailed profile of any user's personal and professional life without ever having read a single word of what they write.

There is a historical example that illustrates this harshly. Former NSA Director Michael Hayden formulated it bluntly in 2014: *"We kill people based on metadata"*. The statement referred to US military operations against targets identified solely by their communication patterns. Not a single message read. Only the contact graph and schedules.

The fact that a service collects metadata does not imply it will use it against its users. It implies it has the capacity to do so, and that a third party with access to that data—by court order, security breach, or sale to third parties if the terms of service allow—also has that capacity.

Access to the Address Book

Another vector that goes almost unnoticed: the contact list. Most messaging services request access to the phone's address book upon registration. They upload all numbers to their server to show who else uses the service. From that moment on, the company has a complete map of the user's relationships, even if the user has never written a single message to anyone.

For a professional bound by professional secrecy—lawyer, doctor, psychologist, consultant—that map contains clients. If the address book has been uploaded to a third-party server, the clients' names are in an infrastructure whose jurisdiction and policies the professional does not control. Professional secrecy is not broken the day someone leaks a conversation: it was broken much earlier, at the moment the upload was accepted.

The Difference Between Encrypting and Not Collecting

Encrypting is protecting content. Being private is not collecting what is not needed. They are different things, and the difference is operationally critical. A service can encrypt all messages perfectly and, at the same time, know almost everything about its users through metadata. The two things are perfectly compatible. In fact, it is the dominant business model in the sector.

The correct question to evaluate the real privacy of a service is not *"does it encrypt content?"*. That question was answered years ago. The correct question is: *"what metadata does it generate and where is it stored?"*. And, above all: *"what metadata does it not need to generate?"*.

An architecture that minimizes metadata by design—not by promise, not by internal policy—is structurally more private than an architecture that collects and encrypts it. Because data that does not exist cannot be leaked, sold, handed over to a court order, or lost in a breach.

For the Professional Reader

If your professional activity involves secrecy, confidentiality, or simply respect for third-party information, it is worth considering the questions in this order:

1. Does the application I use for communication encrypt content? (Probably yes.)
2. Does it encrypt metadata? (Probably no.)
3. Does it generate metadata that it *does not need* to function? (Almost certainly yes.)
4. Where is that metadata stored and under what jurisdiction? (Probably outside the European Economic Area.)
5. Does my client or patient know their data is there?

The last question is the uncomfortable one. Because the honest answer, in most cases, is no.

This article is the first in a series on the actual functioning of professional communication tools. Future installments will address GDPR compliance in messaging and the concept of professional secrecy in the digital era.

Sources and further reading

- Hayden, M. — Statement at Johns Hopkins University, 2014 ("We kill people based on metadata"). Public transcripts available.
- GDPR (EU Regulation 2016/679), arts. 4 and 5 — definition of personal data and processing principles (metadata is indeed personal data).
- EDPS and EDPB — opinions on the processing of traffic data and metadata in electronic communications (ePrivacy Directive).

← PreviousA brief history of wax sealingNext →Professional Secrecy in the Digital Era

Recent readings

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

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 ca16bdc5ff27f95aa5968e87d233165c41f38c718690b301f0ea302f72a0e209

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