



THE LAB · ENTRY 01 · FINDING

The grant is user-shaped, *not data-shaped.*

Connect an assistant to your mailbox and the narrowest permission that lets it read one message lets it read every message. Connect it to your drive and the default search corpus is, in the publisher's own words, files *owned by or shared to* you. There is no supported way to say *my files, except the folder the legal team shared with me*. The unit of restriction is the application. It is never the data.

Edition v1 · 12 September 2026

Live page riskmandate.ai/lab-connector-grants.html

Published by RiskMandate · CC BY 4.0

This is a dated edition of a page that changes. The Lab holds our current thinking, and current thinking moves. This PDF does not: it is what we thought on the date stamped below, kept so the reasoning can be followed rather than only its conclusion. The live page may since have been corrected, extended or withdrawn — and if it has, the edition list on it will say so.

Four scopes, in their publishers' own words.

Each of these was read on 12 September 2026 from the linked page, and quoted rather than paraphrased. Nothing below required an account, a test or a request to anybody's system.

“View your email messages and settings.”

The description of `gmail.readonly` – the narrowest Gmail scope that returns a message body. The only scope that excludes bodies is `gmail.metadata`, described as “view your email message metadata such as labels and headers, but not the email body”, and it cannot read a message. There is no scope that filters by sender, label or date. · [developers.google.com – Gmail API scopes](https://developers.google.com/gmail/api/scopes)

“Files owned by or shared to the user.”

Google's definition of the user corpus – and corpora defaults to user. So on day one, the default search over a Drive grant spans everything any colleague, client or counterparty has ever shared with that person, without anybody choosing it. · [developers.google.com – Drive files.list](https://developers.google.com/drive/api/v3/about-files)

“Site-specific permissioning (using *.Selected permissions) is not supported because the underlying search is tenant-wide.”

Anthropic's security guide for its own Microsoft 365 connector, describing why the narrowing mechanism Microsoft provides cannot be used. The same page states that shared-mailbox access is read-only via `Mail.Read.Shared`, and that the connector uses delegated permissions so a user reaches only data they already have permission for. · [support.claude.com – Microsoft 365 connector security guide](https://support.claude.com/articles/microsoft-365-connector-security-guide)

`account_info.read` · `files.metadata.read` · `files.content.read` ·
`files.content.write` · `sharing.read` · `sharing.write` · `file_requests.read` ·
`file_requests.write`

The eight scopes requested by the official Dropbox MCP server. Two of them are write scopes and two are sharing scopes. There is no folder-scoped variant. · [help.dropbox.com – connect the Dropbox MCP server](https://help.dropbox.com/develop/mcp-server)

The unit of restriction is the application and the tool. It is never the data.

Every lever these products offer turns a capability on or off for an assistant. None of them narrows *which material* that capability reaches. That is the finding, and it is why a behaviour policy for a connector shape is a different document from one for a coding agent: the question stops being *how far can it reach* and becomes *whose material is in reach*.

THE FAIR READING

Nobody is exceeding **your own access**.

This is the objection a vendor would raise first, it is correct, and stating it makes the finding stronger rather than weaker.

- **A delegated connector reaches what you can already reach, and no more.** Anthropic's own guide says so in as many words: users can only access data they already have permission for, and cannot bypass sharing settings or folder permissions. No privilege is being escalated.
- **The problem is not escalation. It is that there is no floor.** Your own access is the *only* boundary on offer. If your mailbox contains a client's confidential correspondence — and it does — then so does the grant, and no setting in any of these products separates the two.
- **Which is exactly what the barrier model already says.** A switch the agent's own account can flip is not a control. A connector toggle you can turn back on in one click is a setting, not a boundary — and the only real boundary available is revoking the whole connector. **The four barriers.**
- **And the default posture is permissive.** On an unconfigured business domain at the largest provider, third-party application access is allowed until an administrator changes it, so a person can connect an assistant to their work mailbox with nobody asked.

THE DEMONSTRATION

In four places, the advertised capability and **the granted scope disagree**.

These are not accusations. Marketing copy and scope lists are written by different people at every company on earth and nothing reconciles them. It is, however, precisely the condition a

behaviour policy exists to surface — so this table is the product's value in one figure.

WHAT IS ADVERTISED	WHAT THE SCOPES IN THE GRANT PERMIT	STATE
Share, move and trash files	The grant's two file scopes are a read-only scope and a per-file scope. Neither authorises acting on a pre-existing file the assistant did not create	unresolved
Create, update and delete calendar events	The publisher's own scope list for that service, as granted, is read-only	unresolved
Label and unlabel mail threads	Neither scope in the published grant authorises label mutation. A <code>gmail.labels</code> scope exists and does permit it — it is not in the grant	unresolved
Search files	Whether the shared-drive parameters are set is undocumented, so whether team drives are in the corpus in practice cannot be determined from the pages	undocumented

These stay unresolved, on purpose.

Each could be settled in an afternoon by connecting an assistant and trying it. We will not: probing somebody else's system to find out what it does is out of bounds here, with no research exemption. An unresolved contradiction, sourced to both of a vendor's own pages and dated, is worth more than a resolved one obtained by poking. If a vendor tells us which page is right, this table changes and says so.

Sources for the table, all read 12 September 2026: [Gmail scopes](#) · [Drive scope classifications](#) · [shared-drive parameters](#) · [the official server's scope list](#) · and the connector descriptions those scope lists sit behind.

WHAT THE MODEL IS MISSING

Reach answers how far. It does not answer whose.

The published capability grammar gives every primitive a reach — `project` , `host` , `tenant` , `world` , `self` — and an `undo` class. Neither says anything about who the material belongs to, and for a connector shape that is the only interesting question.

- `read.record.mailbox` would say the agent can read a mailbox. It would not say that the mailbox contains correspondence from clients who never agreed to any of this.

PROPOSED PROPERTY	VALUES	MEANING
material	OWN ORGANISATION THIRD_PARTY MIXED	Whose material the capability reaches

Almost every connector capability is mixed , and that is the finding.

A mailbox is mixed. A shared drive is mixed. A personal notes folder is own . The value of the property is that mixed **cannot be made own by any setting any of these vendors offers** — which is the user-shaped finding expressed as data rather than as a paragraph, and therefore computable.

This is a proposal against somebody else's published data, not a change we can make. It is written up as a request, with its evidence, at [Lab 03](#).

WHICH LAW REACHES FIRST

Data protection, before the AI regulation.

- A mailbox is mostly other people's writing. A shared folder is mostly other people's files. So a connector grant is, by construction, a grant over material that was entrusted rather than owned — and that is a provision, not an analogy.
- **The sub-delegation provision is one sentence.** A processor shall not engage another processor without the prior written authorisation of the controller, and the first remains liable for the second. Connecting an assistant to a mailbox of client correspondence is that sentence, in the form a stranger already recognises.
 - **Every organisation already has somebody accountable for data protection.** Almost none has anybody accountable for the AI regulation — whose deployer obligations were deferred to 2 December 2027 and reach only systems in the high-risk annex. Mapping to the instrument that already has an owner is the difference between a finding somebody acts on and one they file.
 - **And here is the honest gap.** No regulator has addressed head-on the case of third-party personal data sitting in somebody's mailbox being disclosed to an assistant by that person's own consent. The nearest published hook is a national regulator's January 2026 assessment, which warns about systems connected to databases not needed for their task and flags the difficulty of assigning controller and processor roles through the supply chain. **That is a hook, not a ruling**, and any policy we publish cites it as exactly that.

OPEN

What we cannot answer yet.

Real questions, published so nobody has to rediscover them. If you know the answer to one of these, that is the most useful thing you could send us.

- **A connector that exists and is switched off** is not in the grant today and is one click from being in it. Neither the barrier model nor the label has a place for that state, and it is probably the most common state in any real estate.
- **Does material belong in the shared capability data or in the policy?** It is a property of a capability *in a context*, which argues for the policy. It is reusable across every policy of the same shape, which argues for the data.
- **What does the mandate elicitation look like for a connector?** For a coding agent the mandate is a job. For a mailbox it is closer to a relationship, and nobody has drafted those questions.
- **Who replies if a vendor disputes one of the four contradictions?** The sourcing is theirs and the publication is ours.

If this is your product and we have it wrong, tell us and this page changes, with a line saying what changed and when. We quoted your documentation rather than testing your service precisely so that this conversation could be a correction rather than a dispute.

• Lab 01

This is what the first five policies are for.

Five deployment shapes, each one a document that makes the sentence above visible for a setup somebody actually runs. The flow that produces them — and what buying one would look like — is drawn next door.

```
}());
```