Let’s get started: Protecting Secrets & Data

by **Todd Bailey**
Chief IP Officer &
General Counsel

Trade secrets, proprietary, confidential – there’s no practical difference among these. All involve protecting confidentiality and controlling access.

Protecting secrets can be low cost and requires no formal registrations, making it great for startups. But it is also the hardest IP protection to maintain and enforce in court, because it **requires good habits and daily attention** to protect those secrets.

A secret can be **powerful or weak**. It all depends on 2 factors:

- how well the owner protects it, and
- crucially, how easy the secret is to reverse-engineer or develop independently - because if the secret is easy to figure out, it doesn’t matter how well it is protected.

That’s why strong secrets require the **right kinds of information** and careful consistent protection.

What can be protected?

Any non-public IP (idea, information or data) can be protected as secret. Software code, collected data, hyperparameter selection, parameter weightings, technical specs and pricing are just a few examples.

Secrets are good for protecting:

- complicated, hard-to-reverse-engineer information;
- diverse collections of information, like know-how;
- ideas you can’t (or don’t want to) patent or protect using other IP tools; and
- proprietary data.

Secrets aren’t as good for protecting:

- Simple ideas, or ideas that can be reverse-engineered. So-called secret recipes or secret sauces are usually just marketing legends.
- Foundational IP (at the very core of your business), because if someone else patents it, you will have to stop using it.
- Things you want to be exclusive to you, because secrets won’t stop independent development or reverse-engineering.

How to protect secrets

Protection relies on self-help measures:

- **don’t tell others** unless they need to know;
- store in a safe place, **restricting access**;
- **mark it** “confidential”; and
- if you must disclose, sign an NDA or confidentiality agreement **first**.

Best practices also include keeping a log of what’s disclosed (so you can later prove what you disclosed), and requesting everything be deleted or returned when the NDA expires.

a) Don’t tell others

Secrets are at risk whenever you disclose them to others. The more people who know a secret, the more likely it will leak.

So, the more important the secret is, the fewer people that should be able to access it, and only when they have a genuine need-to-know.

Customers can quickly become competitors, so the less they know, the better. Learn to talk about **what you do, not how you do it**. Don’t be afraid to keep your black box closed. The same goes for talking to **investors**.

Vendors can become leak points. Design your software and processes so that you don't have to give vendors your secrets – **keep the important stuff in-house**, and outsource only routine and mundane stuff.

Employees are also a risk. Yes, they are a trusted resource – but they can also leave to competitors. **Learn to segregate information internally**, using need-to-know, so that your important secrets don't walk out the door every time an employee leaves.

Be wary of JV and partnerships that may just be a **ploy to access your secrets**. As with customers and investors, even under NDA talk about what you do **but not how** you do it. Never provide all the pieces to the puzzle.

b) Store safely & Restrict access

This is where most people are their own worst enemy. The **hardest part** about secrets is the **daily habits** necessary to maintain the legal protection.

The legal system will only allow you to protect as secret **what you actually do protect** as secret. To enforce your secrecy right in court, you have to prove you took all reasonable measures to protect your secrets – **both outside your company and internally**. Far more secrets are lost through mismanagement than through evil actions.

Protection best practices include:

- ❖ Catalogue the most important secrets;
- ❖ Restrict access, **even internally**, using physical and electronic controls appropriate for the importance of the secret; for example:
  - ❖ Protect models, such as breaking them down to reside on multiple servers;
  - ❖ Keep all code on your platform;
  - ❖ Access data through APIs, to avoid disclosing source code;
- ❖ Ensure NDAs are signed before all disclosures; and
- ❖ Disclose only when there is a **need-to-know**, even if there's an NDA.

c) Mark "confidential"

Source code headers, document templates and other secret items should have confidentiality notices to warn others, internally and outside, that the information is secret.

d) NDAs

If you must disclose secrets, a signed NDA is necessary **first**.

Not all NDAs are the same – one-way, two-way, incoming, reciprocal, limited, perpetual – there are many different kinds, and having **the wrong kind can be fatal** to your secrets.

Don't assume that a template you downloaded from the web, or copied from a vendor, is good for your business. A lawyer who understands your business should **prepare a suitable NDA template**. And when using that template, don't agree to changes without fully understanding the effect on your secrets.

Even with a signed NDA is in place, you must continue to **apply the need-to-know principle** to guide you on how much to disclose:

- ❖ Talk about **what** you do, but **not how**;
- ❖ Talk in terms of **user benefits** and advantages, without opening your black box; and
- ❖ If you must open your black box, **open it as little as possible**, and avoid giving anyone all the pieces to your puzzle.

Protecting data

These principles also apply to protecting data:

- ❖ protect with encryption or other means;
- ❖ restrict access using the need-to-know principle;
- ❖ NDAs are essential;
- ❖ don't allow copies to be made;
- ❖ restrict how the data may be used; and
- ❖ revoke access when no longer necessary.

If derived data is created, ownership, access and use should be addressed in a contract. We'll dive into contracts in a future IP WHY episode.