3 Developing an IP Protection Strategy for Your Semiconductor Company – PART II

This Patent Stuff and My Semiconductor Business – Post 3

This is Part II of the second article about patents and chips. In Part I gave an introduction to IP protection, and discussed business concerns and strategies. In this Part II, I discuss details about the tools at your disposal.

This three-weekly series discusses various IP protection aspects from a patent and a business point of view. At the end of the article is a link to the earlier posts. Thanks for reading, and don't forget to give feedback if you read via LinkedIn!

3.1 Keeping Your IP as a Trade Secret

Keeping your intellectual property secret is a great and inexpensive option wherever it is practical (the catch).

If a competitor can buy (or obtain, "find", or steal) your product and reverse engineer it, then keeping your know-how secret may not be a practical option. Say, your chip goes in a cell phone, or a base station, or a door camera, or a drone, or an electric vehicle, then you have no control over where it ends up, and neither do your customers. Anybody can buy the end product, take out your chip and reverse engineer it. A rogue parading as a potential customer may even get samples and other information directly from you.

However, for part of your technology it may be a great option. Particularly for information that doesn't show directly in the end product, or that is very expensive to find by reverse engineering, keeping it secret is a good strategy.

Trade secrets and protected publishing (especially patents) are non-overlapping ways of protecting your know-how. A patent results in publication, which means it is best to employ for innovations that you don't want or cannot keep secret. Of course, you can use the two strategies in a complementary way – patent part of your know-how, and keep another part as trade secrets.

There is one way of keeping secrets that I cannot recommend. If your engineers don't document their work, then there is a natural barrier for their knowledge to spread. I hope I don't need to spell out the pandora box of problems that opens up for your company with this approach. Not to mention the fact that the work may still be copied by a copycat. In the following subsections are details about the tools that you can use to protect your trade secrets.

3.1.1 Non-Disclosure Agreement

Most companies are very used to working with NDAs, and most NDAs that go around today are mutual and reasonably well balanced. An NDA will likely slow down the leaking of your knowledge. However, NDAs don't give absolute protection. First,

one NDA is not the same as the other—not just in the terms, but also in what they protect, and what they oblige each party to do. Unfortunately, in most companies there is a large disconnect between legal staff on the one hand and businesspeople and engineers on the other hand. A lawyer approves an NDA, and an executive signs it. The NDA goes in a drawer or in a file, and the only thing that is ever checked is if it has expired already. The businesspeople don't enforce the specific terms of an NDA; the engineers never even get to see these terms. It is very common for employees of a company that has an NDA with a vendor and another NDA with a partner to disclose vendor information to the partner under the assumption that this is allowed and protected by the NDAs. But this may not be so. Please work with your lawyers, and the involved internal teams to take away this disconnect. And make sure that it doesn't exist with your contract partners either. You may need to proactively enforce each NDA and make it more than a paper formality.

Keep in mind that most NDAs expire. They usually have a clause that says when they expire, your contract partner needs to return all confidential information, or destroy it and certify to you that they have done so. But in practice, have you ever seen it happen? The reality of an NDA is that after several years your secrets may no longer be protected. You may need to think about an NDA's duration. How about 10 years? In my view, 10 years equal two eternities in semiconductor land, and should be plenty. But some foundries have unlimited terms for NDA covering their advanced processes.

Another weakness of NDAs is that reverse engineering by a third party can still expose your secret knowledge.

3.1.2 Circulation Control

Sensitive documents must be limited to those who have a need to know. But a further way of protecting the information is to allow the documents to be accessed only by persons who are authorized and registered. Maintain a list of authorized readers, and make sure that those authorized readers know that they are privileged to be on the list. Obviously, circulation control comes with the burden and cost of bureaucracy. You want to use it for more sensitive information only.

When you have a document with circulation control, make sure its filename is specific for each person on the list, give it a user-specific password and watermarking (see later), and make sure the recipient confirms receiving it.

3.1.3 File Protection

You can protect documents in several ways. Useful options are:

- Password protection for opening a file. A PDF, an MS Word file, and a LibreOffice/OpenOffice Writer file can all be password protected for opening. The file is encrypted, and can only be read when opened with the correct password. You can make the password user specific, destination company specific, or source company specific. Obviously, making it user specific provides the best protection. It works best in combination with circulation control. But it also creates the most bureaucracy.
- Locking a file for editing. Without an author-specific password, the file cannot be modified and re-saved. However, this may provide limited protection. For example, a lock in an MS Word file can be cracked in a fraction of a second. And unless the file is also protected against opening, an unwelcome reader may still learn all its content.

- Disabling copying the text. Again, this should be used in combination with protection against opening the file. If the text can be copied, it can be edited and republished in another document. Even with this protection, a hacker can take a screenshot and feed it to an OCR program to get an editable text.

You may need to do some research to decide how you create PDF files. To create a protected PDF with MS Word, use CutePDF Writer (downloadable for free). If you use LibreOffice Writer, or OpenOffice Writer, both excellent and free alternatives to Word, then you will have the option to directly export your file to PDF. They offer the security features in Figure 3.

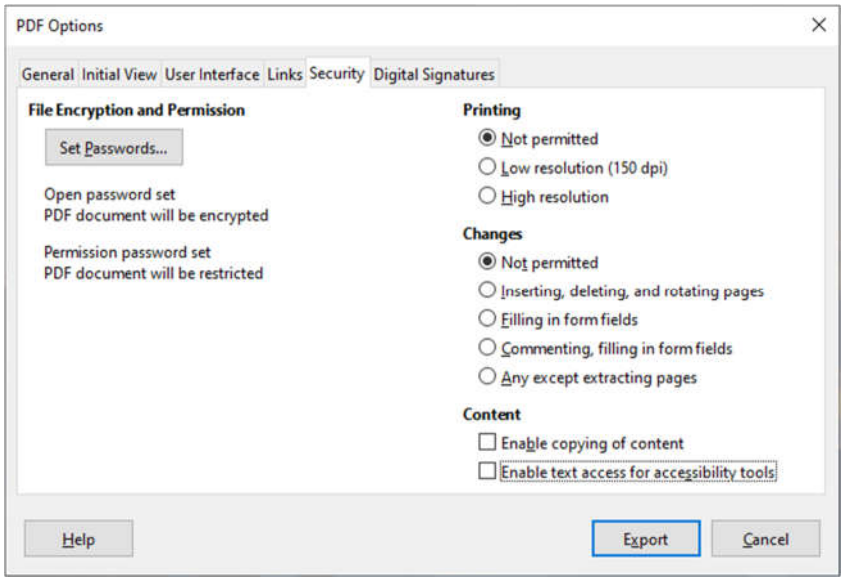

Figure 3 - PDF security features offered by LibreOffice.

As you can see, it allows you to restrict printing, changing the document, and copying.

PDF documents that are unprotected and that contain text may be opened in MS Word and other editors. Hackers can also remove watermarks, at least the ones they are aware of. But very few people would go through many steps when stealing your technology, so it is still a barrier that you want to raise.

3.1.4 Watermarking

You may further protect your confidential documents, especially those that you provide in PDF form, with watermarks.

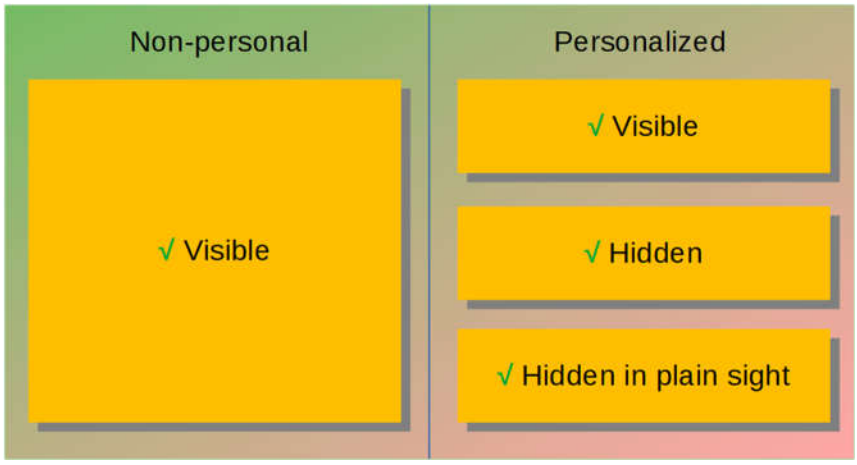

Figure 4 - Types of watermarking

They can be non-personal or personalized, and there are watermarks that are visible, hidden, or hidden in plain sight (see Figure 4). A visible watermark can be a picture or text in the background, usually something like "Confidential", but it can also be a line in the footer or header that identifies the information as confidential, and that may further identify the intended user. A user who sees his name on every page in a document may be less inclined to provide copies of the document to others.

Figure 5 - A personalized visible watermark in a document footer or header

Non-visible watermarks are also useful to identify the user, but of course they only deter if the user knows (or suspects) that you are using them. Equally useful are personalized watermarks that hide the information in plain sight. Those embed for example digital information in any number of ways, like by inserting meaningless words or phrases, or by selecting between or among synonyms. In "The actual car may be a large vehicle or a truck", the word *actual* is meaningless and could be left out. Its inclusion may encode one bit. The words *car* and *vehicle* are synonyms, so their two occurrences can encode two bits. *Truck* could be replaced by *big rig*, giving another bit. Thus, this short sentence could encode four bits of information in plain sight, and the four bits could identify a specific user out of a list of sixteen. Creating a watermark like this by hand may be time consuming, but both MS Word and LibreOffice/ OpenOffice can work with macros that can make the task nearly effortless. By the way, relevant information can also be hidden in fake information, and in internet links. If you want to tease yourself, read the paragraph in the sidebar, which identifies user number 13 of 32.

Hidden in Plain Sight

This paragraph identifies one out of 32 users. It can be about any subject, and still provide the information, which needs just 5 bits. This paragraph is called a **key section**, i.e., a section of your document that holds a set of **dummies** (meaningless words and/or phrases). Dependent on a number that you encode (the user's list index, a number up to 32), some of the dummies show, and others don't. You could of course have 32 dummies, but you need only 5 to encode 5 bits, or 32 possibilities. So how does it work? Here is your first clue: a dummy may or may not be totally meaningless words. Like the word "totally" in the previous sentence. Each dummy can represent one bit. If it isn't there, the bit is 0, and a reader couldn't even know it. The dummies don't actually need to be the same. You can even put in, or not put in, this sentence. Did you know that room temperature, for electronics people is 27.13 degrees Celsius? Well, it isn't, because that information is partially false. It could be anywhere in the range of 20 to 30 degrees or it could be 300K (26.85 Celsius), but it hasn't actually been defined. Or, you can use fake links, like http://fakeascanbe.com/search?page=13_&fakeinfo=3762. You got it? Which unlucky user do you think we identified?

Watermarks require that when things go wrong you can get your hands on a leaked document. So, if you are using a personalized watermark in your confidential datasheet, then it is useful to provide a visible watermark, an invisible watermark, and to notify the reader in the document, for example as shown in Figure 5.

So how does an invisible watermark work in a text document? One way is to add watermark information by modulating spaces and line heights. If you encrypt the hidden information and add error detection and correction, it becomes hard to tamper it. With the naked eye it should be difficult to see that there is something there. With specialized reader software

an adversary can extract the modulation, but without the decryption password he'd still know nothing. So, did you notice that your name (and that of your secret lover) is hidden in the spaces in this section? Did you even see that the words and lines are dancing around a little bit? OK, I'm appealing to your personal paranoia, but I hope you got the point.

Use watermarking in combination with an NDA, circulation control, and file protection.

3.2 Publishing Your IP

Publishing can be a strategy when you can't keep something out of the hands of bad actors in every way, like when your product can be reverse engineered. Or when you want to publish for marketing purposes. There are a couple of tools available that give different levels of protection and that suit different situations.

3.2.1 Copyright

Copyright is an inexpensive way to protect your software and firmware code, your RTL source code, your design source files and documentation, test and calibration source files and documentation, datasheets, etc. Copyright protects original works of authorship, for both published and unpublished works. You don't have to register, unless you plan to sue somebody for infringement. Register before the infringement begins, and you may be entitled to claim statutory damages and attorneys' fees in your infringement lawsuit. You can learn (much) more at www.copyright.gov. You can register your work through the electronic Copyright Office (eCO). But note that even online registration still requires that you submit a hard copy of the work.

Make sure to have your engineers include copyright claims, confidentiality statements, and even basic license information in any documents that are released to customers. Make sure that you know what is in these inclusions—don't leave it to your engineers to imagine what they could write there. It is not their job to figure it out, and they haven't been trained for it (I would guess). Work with your lawyer to determine a text that your engineers must include in their files and/or documents. Then instruct them to include it, and regularly verify that they actually do so.

Copyright, in many countries, gives a long protection. However, it is not necessarily a strong protection. Some of your information, like datasheets and PowerPoint presentations, will easily end up with competitors, even with the added protection of an NDA. To stop a copycat, you may have to hire expensive legal representation in a foreign country. A bad actor may audaciously get away with stealing and abusing your information. Use copyright wherever possible, and in confidential documents, and expect its protection to be best when the spread of information is limited and in your control.

3.2.2 Mask Registration

The **Semiconductor Chip Protection Act of 1984** (SCPA) was instated in the US to protect the layouts of integrated circuits upon registration. If you have registered your "mask works", nobody may copy them without your express permission. (It is not illegal to reverse engineer your layout, though.) Registration (in the US) is at the Register of Copyrights, and protection lasts 10 years (two eternities). Many other countries have followed the US, and instated similar laws. If you want to learn more, good overviews are on Wikipedia and the WIPO website.

3.2.3 Patent

A patent publishes your invention for the whole world to see, and it gives you a privilege, in exchange for which you give your invention to the public after 20 or 21 years. Your privilege is that in the country that issues the patent you will have the right to stop others from producing, selling, or using the invention. There are at least 195 countries in the world today, so if you patent in one or two countries, there are at least 193 countries that don't give you that privilege. You will have to decide: would it make a difference if you didn't patent your 6G communication processor in Somalia? Or Sweden, for that matter? (Stop here for a bit, and think about Sweden.) I'll discuss your choice of countries in the next post.

Lastly, let's remember for what types of innovation a patent is useful. As I mentioned earlier, if the invention can be reverse engineered from your product, or read from your datasheet, or understood from your presentation at ISCC or DAC or your article in JSSC, then a patent can provide protection. Your architectures, circuits, devices, and also proprietary foundry processes are all good candidates for patent protection. Protection start at the day of issuance, but is effective as of filing.

Upcoming:

4 In What Countries Should I Patent, Anyway?

5 Choosing the Right Patent Person for Your Inventions

6 How is a Chip or Firmware Patent Different than Other Patents? What About a Software Patent?

7 Woohoo! I Invented a Huge Improvement over My Competitor's Invention!

Posted so far:

1 So You Got This Great Idea That Will Wipe Out Competition. Now What?

2 Developing an IP Protection Strategy for Your Semiconductor Company – PART I

3 Developing an IP Protection Strategy for Your Semiconductor Company – PART II

Disclaimer

Please do not construe anything in this article as legal advice: it isn't. The article contains my private opinions, with where possible the point of view of a semiconductor industry entrepreneur and/or a patent agent fighting for the inventor and the entrepreneur. If you need a strong patent on your circuit and/or system, I might be your guy.

www.icswpatent.com