自主开发规划

2024-08-01

| 作者：詹姆斯·普利 (James Pooley)
| 译者：孙惠平 北京天驰君泰律师事务所

“逆向工程的“净室”规则被视为黄金标准.....但问题是，由于多种原因，真正的“净室”往往是不切实际的。”

“The gold standard[1] is the ‘clean room[2]’ form of reverse engineering[3]... The problem is that a true ‘clean room’ is often impractical for a number of reasons.”

“非同凡想”[4]

— 1997年Apple Mac 广告活动

无论故事的主人公是公司离职的高管、还是公司的客户或商业伙伴，故事的每次发展似乎都千篇一律：这类曾长期与公司分享机密信息的“演员”，他们跳槽后的公司发布了与原公司类似的产品，原公司都会声称被盗、被背叛、被出卖，而“演员”的反应同样强烈：“不，我是自己做的”；用法律术语来说，“我从事的是'自主开发'”。

The story seems to unfold the same way every time, whether the actor is a high-level departing employee or a customer or business partner. When sharing confidential information in a long-term relationship results in the release of a similar product by the recipient, the reaction is a claim of theft, laced with accusations of treachery and betrayal. And the response is equally strong: “no, I did this on my own”; in legal terms, “I engaged in‘independent development.’”

严格来说，很难证明新产品的开发是“独立”于保密关系中获得的信息完成的。一旦你接触到了保密的程序或设计或其他相关信息，你如何证明你的工作完全是你自己做的？

Strictly speaking, this means that the development of the new product was accomplished “independently” of the information shared in the confidential relationship. As a practical matter, this can be difficult to prove. Once you have been exposed to the secret process or design, or other related information, how do you demonstrate that your work was entirely your own?

对于那些希望通过收购来扩大业务的公司或者对于那些对创新途径保持开放、寻求与创新型企业建立合作，共同研发新技术的公司而言，，这都是一个特殊的难题。《华尔街日报》近期的一篇文章报道了一个系列案件，苹果公司在与某些初创企业就iPhone和Apple Watch的相关技术进行洽谈之后，却最终选择独立推进这些技术项目，从而引发的一系列法律争议。

This is a particular conundrum for companies that are looking to expand their business through acquisitions, or who respond to inquiries from an innovator interested in some sort of relationship to co-develop a new technology. A recent article in the Wall Street Journal reported on cases where Apple met with startups to look at technology related to the iPhone or Apple Watch, and the legal battles resulting from Apple’s decision to pursue those projects on its own.

1 “残留记忆条款”[5]

The ‘Residuals Clause’

大公司通常会在与小公司的协议中加入“残留记忆条款”来保护自己免受这类诉讼。协议中除了通常的保密承诺和有限使用共享信息外，还加入了“被无意识保留的信息”的例外情况，即该信息已被融入了相关人员的记忆中。如果你觉得这是一个重要的例外条款，那就对了。实际上，签订带有残留记忆条款的协议，意味着你授权对方利用在交易过程中所记住的任何信息。

One way that a large organization can try to protect itself from these claims is to insert a“residuals clause” into the agreement with the smaller company. Alongside the usual promises of confidentiality and limited use of shared information it inserts a significant exception for information “retained in the unaided” (i.e., human) memory of the individuals who were exposed to it. If that strikes you as a significant carve-out, you’re right. In effect, by entering into an agreement with a residuals clause, you’re granting a license to the other side to use whatever they remember from the transaction.

因此，残留记忆条款经常遭到拒绝，在此过程中，各方都会签署一份相对标准的保密协议，同意对信息进行保密并同意仅将该信息用于评估拟议的交易。接收信息的公司可以在协议中声明自己正在进行相关研究，从而在一定程度上降低风险。但即使有这样的免责声明，也会接触到一些信息，从而给日后证明真正的自主开发带来挑战。

As a result, the residuals clause is frequently refused, and the process goes forward with a more or less standard NDA in which each side agrees to maintain information in confidence and to use it only to assess the proposed deal. The receiving company may reduce its risk to some extent by declaring in the agreement that it is engaged in its own related research. But even with that sort of disclaimer, there will be exposure to information that makes it a challenge later to demonstrate truly independent development.

这样的接触并不仅仅发生在潜在的收购或许可中。在购买商品时也可能共享机密信息，因为销售条款包括对卖方设计的保护。同样的情况也可能发生在企业软件上，客户虽无权访问源代码，但也会接触到有关该软件如何工作的信息，通常还要求承诺不对该软件进行逆向工程。当然了，保密信息有时依然会在竞争对手雇佣的工程师的头脑中闪现。

An exposure like this doesn’t only happen in the case of potential acquisitions or licenses. Confidential information can be shared in connection with purchase of a commercial product, in which the terms of sale include protection for the seller’s designs. The same might apply to enterprise software, in which the customer is not given access to underlying code, but is exposed to information about how the tool works, usually accompanied by a promise not to reverse engineer it. And of course sensitive information sometimes arrives in the head of an engineer hired from a competitor.

无论如何，“信息感染 ”或多或少都会以某种方式限制信息接收者的自由。这种限制可以用出现某种索赔的风险来衡量，也可以用接收者事实上并没有使用其秘密接收到的信息这种强有力的证据来衡量。

However it occurs, the “information infection”[6] operates more or less automatically to constrain the recipient’s freedom in some way. That constraint can be measured by the risk that there will be some sort of claim, and by the robustness of the evidence that the recipient did not in fact use the information it received in confidence.

2 盗用不必要求抄袭

Misappropriation Does Not Require Copying

在商业秘密被盗用的法律争议中，无需证明对方抄袭，关键的因素是“使用”。如果某方的后续开发工作受到之前获得的机密信息的影响，或者获得该信息只是在某种程度上加速了其开发进程，法律则对此苛以责任。此外，如果一方使用了原创者之前通过研究和资金投入所获得的有关哪些方法无效或效果不太好的“负面秘密”，则同样构成对商业秘密的使用，即使这些负面秘密揭示的是失败的尝试，它们作为达到成功目标的基础，往往具有不可小觑的价值。正如托马斯•爱迪生在描述其为了发明耐用的电灯丝所付出的努力时所言：“我并未失败，我只是找到了一万种行不通的方法”。

The key word here is“use.”To assert a claim of trade secret misappropriation, you don’t have to show copying. The law imposes liability if the later development was influenced, or just accelerated in some way, by access to confidential information. This includes

using knowledge of the blind alleys[7] already explored by the originator who invested in research to determine what doesn't work, or what works less well. These so-called "negative secrets" can be very valuable as a "head start" toward success. Recall that Thomas Edison, in relating his effort to invent a long-lasting filament for the light bulb, said "I haven't failed; I've found 10,000 ways that won't work."

在涉及违反保密义务的纠纷中，原告总是负有"举证责任"，即原告必须说服法官或陪审团其秘密被盗用。但实际上，如果被告方曾拥有对机密信息的正当访问权限，并且此后推出了类似的产品，那么被告方将成为审判焦点所在，此时被告方最好讲好一个有说服力的辩护"好故事"。

In a dispute over breach of confidentiality, the plaintiff always has the "burden of proof," in the sense that it has to convince the judge or jury that its secrets were misappropriated. But as a practical matter, if the defendant had trusted access and later sold a similar product, all eyes will be on the defendant, who better have a good story to tell.

正如我们在文章开头所指出的，这是一个"自主开发"的故事。。但是，被告该如何说服（可能持怀疑态度的）受众相信不存在失信行为，其开发是"干净的"？

That story, as we noted at the beginning, is one of "independent development." But how does the accused convince a (potentially skeptical) audience that there was no breach of trust, that the development was "clean?"

"逆向工程的"净室"形式被视为黄金标准。在此原则下，你将有关某款产品的公开信息或基本规格信息交给从未接触过秘密信息的外部开发团队，让他们以此为基础进行开发。当然，你必须确保所有参与者都是"干净"的，你给他们的信息不是来源于商业秘密。一旦你能做到这一点，你就赢了。

Here, the gold standard is the "clean room" form of reverse engineering, in which you start with publicly available information about a product, or a set of basic specifications for a desired product, and you hand that over to an outside team of developers who have never been exposed to the secret information. Of course, you have to be certain that all the participants are clean, and that the information you give them to start with was not derived from the trade secret. But if you can pull that off, then you should win.

3 "净室"可能不切实际

A 'Clean Room' May Not Be Practical

问题在于，出于种种原因，真正的"净室"往往是不切实际的：可能受限于时间或预算的限制、可能难以在需要时聚集具备合适技术专长和经验的开发团队、甚或因为涉密信息被暴露的程度相对较低，使得相关风险被视为在可控范围内。

The problem is that a true "clean room" is often impractical for a number of reasons. There may not be enough time, or enough budget. The people with the right skills and experience may not be available when needed. Or the extent of exposure may have been so limited that the risk is viewed as acceptable.

事实上，风险评估对大多数自主开发至关重要。接触敏感数据的公司必须明白，风险评估并不是非黑即白的，而是依赖于周到的风险管理，从建立关系并接收保密信息之初就开始实施的风险管理。考虑到需要举证证明自主开发，信息的接收方尤需关注在被起诉时，如何保留其选择权[8]。

Indeed, assessing the risk is key to most attempts at independent development. The company that is exposed to sensitive data has to recognize that the issue is not clean-cut, but depends on thoughtful risk management, beginning at the point when the relationship is established and the information received. Anticipating the practical burden of proving independent development, the recipient will focus on ways to preserve its options in the event of a claim.

这项工作始于交易之初。如果公司正进入一段保密义务关系，那么合同起草时就应向另一方明确表示，如果事情没谈成，信息接收方将自行推进。对所有机密信息进行具体标注的条款（以及对口头披露信息的及时书面确认）将有助于降低对受保护信息内容的误解风险。

This effort begins with the originating transaction. If the company is entering into a confidential relationship, the contract should be drafted in a way that makes it clear to the other side that if things don't work out the recipient will be forging ahead on its own. Provisions for specific marking of all confidential information (and prompt written confirmation of verbal disclosures) will help reduce the risk of misunderstanding about what the protected information consists of.

对于招聘过程中涉及的泄密风险，用人单位应明确其尊重他人知识产权的政策，并应考虑建立制度来指导新员工和与其接触的老员工的行为。在特殊情况下，公司可能希望通过独立律师来为个人提供具体的、保密的指导。

For recruiting exposure, the hiring company should make clear its policy on respecting others' IP, and should consider establishing protocols to guide the behavior of new recruits and their new colleagues. In exceptional cases, the company may want to provide access to independent counsel to provide the individual with specific, confidential guidance.

如果没有后续措施跟进，以确保泄露风险得到很好的管理，并且做好公司履行义务的记录，来证明公司是如何遵守其义务的，那么所有这些前期的行动可能都无济于事。

All this front-loaded action may not help much without follow-up to ensure that exposure is carefully managed and that good records are kept of how the company has complied with its obligations.

4 构建自主开发工作

Structuring the Independent Development Effort

那么，在接触了他人商业秘密的情况下，如何构建一个独立开发路径呢？首先要认识到这并不一定需要一个密闭的 “净室”。即使有一名或多名接触过敏感数据的人员参与，你也有可能“自主地”创建自己的产品或服务。但出于显而易见的原因，你应当将这类人的工作限制在必要的范围内。法律仅惩罚那些“实质性”的滥用行为，而且根据具体情况，你也许可以说服法庭，那些因接触保密信息而造成的任何影响都是微不足道的。

This brings us back to the question of how to structure a development path when there has been some exposure to someone else's trade secrets. The answer begins with recognizing that it doesn't necessarily require a hermetically sealed "clean room." It is possible to create your own product or service "independently" using one or more of the people who had access to sensitive data. For obvious reasons you should limit their participation to what is necessary under the circumstances. But the law only punishes a misuse that is "substantial," and depending on the context, you may be able to convince a court that any influence from exposure to confidential information was negligible.

成功的关键在于洞悉未来可能面临的诉讼风险，并妥善保存好工作记录。对于法官或陪审团而言，这一点显得尤为重要，因为他们需要清楚地看到你的开发工作是稳健而诚实的，你必须证明，你没有试图通过回避他人已完成的研究或实验来寻求捷径。为了证明你的工作确实是基于你自己的独立思考和努力，而不是仅仅依赖于从他人那里学到的知识，你需要精心规划你的开发路径，就从“非同凡想”开始吧！

The key to success lies in understanding the risk of future litigation and preserving the evidence of your work. This becomes critical as context for a judge or jury to see that your development effort was robust and honest, and that you didn't cut corners by avoiding the research or experimentation that was already done by others. To show that what you did was "independent" of what you learned from someone else, you should frame your plans accordingly. Begin by thinking different.

[1]译者注：黄金标准法则，在品牌定位和广告表现上，为品牌设立一个可使之与同类品牌相比更加出色的说辞，从而体现出该品牌的高出一等，胜人一筹；黄金标准可凸显品牌的优越品质、独特利益和全新价值，使品牌的销售主张（USP）更有表现力、冲击力、说服力和促销力。摘自MBA智库.百科.黄金标准法则

[2]译者注：clean room净室。参考Understanding The Digital World --What You Need to Know about Computers,the Internet,Privacy,and Security,Second Edition by Brian W.Kemighan【美】布莱恩.W.柯尼汉 著《普林斯顿计算机公开课》（原书第2版） 戴开宇 译 5.4.3版权“.....技术上这叫净室开发(clean room development)，也就是说，程序员完全没有接触或者不了解自己正在仿制软件的代码。虽然他们自己写的新代码与原始程序有相同的行为，但是可以证明没有抄袭。这样，法律问题变成了证明洁净室确实是干净的，没有人因为接触过原始代码而被污染.....”

[3]译者注：reverse engineering逆向工程。参考《逆向工程技术综合实践》 成思源主编 电子工业出版社 2010-10月出版。第1章 绪论“传统的产品实现通常是从概念设计到图样，再制造出产品，我们称之为正向工程，而产品的逆向工程是根据零件（或原型）生成图样，再构造产品...逆向工程的重大意义在于，它不是简单地把原有物体还原，而是在还原的基础上进行二次创新...逆向工程技术已广泛应用于产品的复制、仿制、改进及创新设计，是消化吸收先进技术和缩短产品设计开发周期的重要支撑手段。”

[4]译者注：Steve Jobs by Walter Isaacson《史蒂夫.乔布斯传》【美】沃尔特.艾萨克森 著，扉页--The people who are crazy enough to think they can change the world are the ones who do.

——Apple's “Think Different” commercial,1997

那些疯狂到以为自己能够改变世界的人，才能真正改变世界。

苹果“非同凡想”广告，1997

[5]译者注：摘自2017年10月31日，商务部中国保护知识产权网《知识产权协议和保密协议中的残留记忆条款》：“残留记忆条款（residuals clause）是知识产权协议或保密协议中的一项条款，该条款规定如果一方（接收方）与另一方（披露方）合作时知晓了后者知识产权的一般信息（general information），则前者可以在不借助辅助手段的情况下使用记忆中留存的信息，而不用顾及协议中的保密限制或者禁止使用限制。

支持残留记忆条款的依据是很难区分从每一个业务合作伙伴那里掌握的一般信息与之前已知的信息或为他人或者内部开发的知识产权。例如，尽管软件开发公司可能不会使用其为客户编写的特定代码，但是对这些软件开发公司来说，很难将为该客户编写代码时掌握的一般方法与其自己的方法或者与其他客户合作时掌握的方法区分开。”

[6]译者注：infection 英文的意思是A disease that can spread from one person to another through direct or indirect contact.一种可以通过直接或间接接触从一个人传播到另一个人的疾病，即感染、传染。这里以“信息感染”形象地说明了那些接触到保密信息的人很难证明自己没有使用或泄露保密信息，即一旦被“信息感染”，开发者很难自证清白。

[7]译者注：根据剑桥英语词典，blind alley---a situation or method that is not effective or will not produce results无效或不会产生结果的情况或方法。汉语俗称为“死胡同”。

[8]译者注：选择权，通常指合同中约定的当事人可以解除或撤销合同等的选择权。

*本文由北京天驰君泰律师事务所国际业务专业委员会高级合伙人朱尉贤律师、陈哲远律师审校。

来源：

作者：斯·普利 (James Pooley)

相关标签

国际业务