The Art of Reverse Engineering

November 15, 2017 by James Pooley

Recently a client asked me for advice on setting up a “reverse engineering” project. The company had just hired a senior engineer from a competitor that had pulled ahead of them the year before with the release of a next generation product. They needed to respond soon. The new employee was “clean,” they assured me, having come over without any documents or files. So they proposed to get him going with a small technical team and some samples of the competitor’s product. He no longer had access to any trade secrets of his former employer; what could possibly go wrong?

In the world of trade secrets, reverse engineering is universally embraced as acceptable. It involves starting with a publicly available product or set of information and taking it apart to discover how it was created. Why does anyone do this? To discover, legitimately, a path already taken:

- to learn, as when a child takes apart a clock
- to change or repair a product
- to provide a related service
- to create a compatible product
- to create a competitive product

In most circumstances, there is nothing wrong with reverse engineering. The recently-enacted Defend Trade Secrets Act declares that it cannot be an “improper means” of acquiring information. (In fact, if you properly reverse engineer a product, the information you discover can be held by you as your own trade secret.) The reason behind the rule is apparent when you consider the limits of trade secret protection: selling a product that reveals the design and method of its manufacture means the secret is imperiled. If it is very easy to discern, then the secret is lost immediately. If it might take some time to figure out, then that’s called reverse engineering, and anyone is allowed to do it.

Like most rules, this one has its limitations. You can’t use the reverse-engineering process to “discover” and duplicate a patented invention. That is one of the advantages inherent in using patent protection instead of trade secrets. Also, if you haven’t simply purchased the product on the open market, but have acquired it by some form of limited license or other

contract that restricts your rights to reverse engineer, the courts normally will enforce those restrictions. Finally, you can't through reverse engineering simply duplicate a product that is protected by a trademark or otherwise market a product so identical that the public would be confused about its source. Indeed, that conduct deserves the derisive label "knocking off."

But to appreciate the potential of reverse engineering, consider the case of Chicago Lock Co. v. Fanberg. For fifty years the Chicago Lock Company had marketed its special "Tubular Ace" lock, frequently seen on vending machines where maximum security is required. In order to achieve that level of security, the manufacturer would provide a duplicate key only to an owner registered with the company. The codes necessary to duplicate the keys were strictly controlled. Lost keys could only be replaced by the manufacturer or by a locksmith who could "pick" the lock to discover the appropriate configuration and grind a duplicate tubular key.

Locksmiths typically would record the relevant "key code" along with the serial number of the customer's lock, to be able to duplicate the key if it was lost again. Fanberg, a locksmith himself, advertised for other locksmiths to provide him with correlations they had recorded over the years. He then compiled all of the correlation codes into a manual and offered it for sale. Chicago Lock Company, understandably upset that its security system was jeopardized, filed a lawsuit.

The court directed judgment for Fanberg. Whatever claims the owners of the locks might have had against their locksmiths for divulging the codes, the manufacturer had sacrificed its products to the possibility of exactly the kind of reverse engineering that occurred. The court explained:

"It is well recognized that a trade secret does not offer protection against discovery by fair and honest means such as by independent invention, accidental disclosure, or by so-called reverse engineering, that is, starting with the known product and working backward to divine the process, Thus, it is the employment of improper means to procure the trade secret, rather than mere copying or use, which is the basis of liability."

If you intend to reverse-engineer a product, however, be careful how you do it. Acquire the product through a simple purchase. Make sure that there are no conditions attached to the purchase that might prohibit you from

reverse engineering. In addition, beware of documentation that is provided as part of the sale that may itself contain confidentiality restrictions. This situation occurs frequently with sophisticated equipment accompanied by maintenance manuals or circuit diagrams with restrictive legends. It also comes up in the disassembly of software acquired under license agreements, where issues of copyright infringement may require special legal advice.

Carefully choose the team that will perform the reverse-engineering tasks. Use only those who have had no exposure to the way it was originally designed and made, and be sure that the team does not have access to any confidential material of the original manufacturer. Maintain detailed records of the entire process, so that it can be demonstrated – to the satisfaction of someone with a technical background – that the process was accomplished “from scratch” and without reference to any restricted information.

As for my client who hired the competitor’s engineer, they agreed they were asking for trouble by involving someone who had previously worked on this technology. Since he was already on board, and as extra insurance against a later claim, they abandoned their internal project and contracted with an outside vendor to perform the work in a “clean room” environment (a term borrowed from semiconductor processing, where particle contamination is strictly controlled), with nothing to refer to but the product itself. Reverse engineering may sound good, but as in so many other areas of trade secret law, the right answer isn’t found in a phrase, but in practical risk management.

www.pooley.com