INNOVATION COUNCIL

Trade secrets and the Internet of Things (IOT)

by Phil Wadsworth

Trade secrets are a form of intellectual property (IP). In order to understand the relevance of trade secret protection to IOT devices, it is helpful to explore the underlying technologies associated with those devices. This will help the reader to appreciate both the benefits and limitations of trade secret protection.

Trade Secrets

The primary goal of a trade secret is to prevent valuable technical or business information, that provides a competitive advantage, from being accessible to the public and competitors. Trade secret protection is lost once the information is generally available to the public and competitors.

Most countries provide some form of legal protection for confidential information, including trade secrets. Trade secrets are a form of unregistered right, meaning there are no formalities (or associated costs) required by a government intellectual property office to secure this type of protection.

Trade secret programs are set up within organizations for the sound management of business confidential information that can be protected as trade secrets. Such programs identify confidential technical and business information, and ensure that non-disclosure agreements are in place when sharing such information with potential partners, suppliers, and others. They also ensure that employee contracts contain clauses obliging staff to maintain the confidentiality of any sensitive technical and business information they come into contact with at work.

The benefit of a trade secret is that the information being maintained in secrecy typically provides the owner a competitive advantage in the marketplace. A technical example of a trade secret is a manufacturing process that improves the quality of the end-product over other similar competitive products. An example of a business-related trade secret is a marketing strategy that results in increased sales of products over other competitive products.

The limitations of trade secret protection must also be understood. In this regard, the implications to trade secret protection for technologies included in a product being introduced into the market place should be considered. Once a product is sold, it can become subject to reverse engineering thus resulting in access to, and utilization of, the trade secret by others. Once this occurs, the value of trade secret protection is greatly diminished, if not totally eliminated. From a risk perspective, it is typically easier and less expensive to reverse engineer software implementations than hardware implementations. If the risk of reverse engineering is high, then patent protection should be considered instead of, or together with, trade secret protection.

IOT Devices

Simply put, IOT devices include any devices that communicate through the internet with each other. They include mobile phones, laptops, vehicles, home appliances, electric consumption meters, and even things like electronic dog collars. Access to the devices by mobile phones and laptops is typically done through wireless technologies such as Bluetooth, WiFi, and cellular technologies known as 4G, LTE, and 5G. Thus, generally speaking, there are two primary technologies included in each IOT device; first is the wireless technology that allows access to the internet, and second is technology that provides the desired functionality for a particular device. Both of these technologies are essentially implemented through electronic processors and associated software.

Wireless technologies are highly standardized, so the higher-level technical specifications and protocols prescribed by the relevant standards bodies must be followed by all product manufacturers that wish to sell standards-compliant products. However, for the most part, the specific implementation of those specifications and protocols are left to each product manufacturer. So to the extent that trade secret protection is being considered for those product implementations, the aforementioned limitations of trade secret protection should also be considered.

The underlying functionality of a particular IOT device is conducive to unique technical implementations. Those implementations can certainly be considered for trade secret protection, but a risk assessment should be considered based on the viability of potential reverse engineering (i.e. the time and cost of reverse engineering).

Steps that governments can take to improve the formal IP system include improving patent quality, ensuring that IPRs and their enforcement are not overly expensive, facilitating patent filing and prosecution by SMEs, instituting outreach and training programs for SME business leaders, making it easier for SMEs to successfully litigate when faced with infringement, and enacting modern trade secret laws.

Actions that governments can take to catalyze innovative interactions include supporting the establishment of innovation networks and geographical "clusters", where innovative activities in relation to specific sectors are concentrated. Governments can also develop frameworks that enable the patenting and licensing of publicly-funded research (and that enhance collaboration between the private sector and public research institutes), and can support the creation of incubators that offer support (such as coaching on business skills and IP management strategies) to SMEs. In addition, governments can also adopt the strategy of directing funds towards technology solutions that have already been appropriately protected.

Summary

Trade Secret protection is especially well suited for manufacturing processes and business practices that can be easily shielded from the public and competitors. However, trade secret protection for technical implementations in products must be assessed, based on the risk of disclosure by way of reverse engineering. The time and cost of reverse engineering should be estimated as part of the risk assessment. A cost/benefit analysis of trade secret versus patent protection, or analysis of the optimal mix of the two approaches, should also be considered.