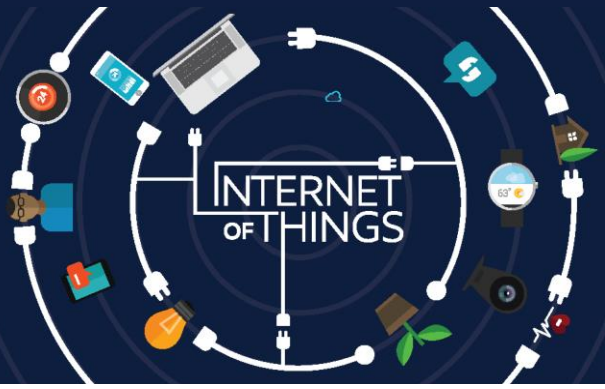

PART 1

CONSIDERATIONS FOR IoT TECHNOLOGY LICENCE AGREEMENTS

AUTHOR // PETER KARCHER

AUGUST 2016

This article originally appeared in the Internet Law Bulletin Vol. 19 No. 5-6 (August 2016) published by LexisNexis

KEY TAKEAWAY POINTS

- The Internet of Things ("**IoT**") refers to the network of interconnected physical devices and equipment, in which those devices are capable of collecting, sending and receiving data autonomously, predominantly via wireless communications.
- The integrated nature of IoT technology, which generally comprises multiple interacting products and services, raises particular issues when considering licence agreements for such technology.
- Licensees should closely consider what contractual warranties a technology licensor is giving in respect of both hardware and software components of the IoT system, and what rights the licensee has if the technology falls short of expectation.
- IoT technology, by its nature, involves the operation of physical objects and human interaction with, and reliance on, those objects. IoT technology therefore carries the risk of personal injury or property damage if the technology malfunctions, so liability for defects, limitations of liability, indemnities, and insurance coverage all require particular scrutiny in IoT licensing arrangements.

WHAT IS THE *INTERNET OF THINGS?*

I recently moderated a forum on the theme of *Succeeding in a Digital Economy* attended by over 80 clients and guests of my firm. In the course of my introduction I asked the audience whether they were familiar with the term "Internet of Things". Surprisingly very few were, although I suspect that, like "New Media", "Tweet" and "#Hashtag", that will not be the case for very much longer.

Essentially the Internet of Things refers to the network of interconnected physical devices and equipment (other than computer terminals themselves) which is capable of collecting, sending and receiving data autonomously, predominantly via wireless communications.

The term has in fact been around since 1999[1], and most people will have already experienced the Internet of Things, or at least read about it conceptually. Driverless cars, Fitbit® watches, and smart thermostats are examples of IoT technology.

On a larger scale, the IoT is creating "Smart Cities" which embody intelligent traffic control and street lighting systems, pollution sensors, and efficient parking grids[2]. In industry, agriculture and construction, IoT technology is allowing business owners to better monitor, sort, collate and view data on assets such as machinery, crops and buildings. Experts differ on the current scale of the IoT,

however there are estimates that between 20 and 50 billion objects will be part of the IoT by 2020[3].

For simplicity, this article considers a typical IoT scenario in which a particular technology is integrated into a device to allow it to collect and record data about the functioning of the device, and to send that data and receive other information. By being able to send and receive data, the device can be monitored and controlled remotely.

A particular technology licensor will have a core proprietary technology, which may in the form of a chipset or module designed to be incorporated into a newly manufactured or existing product, or piece of infrastructure. The licensor may have proprietary firmware (embedded software) as part of this base technology. A product specific interface may need to be developed in order to get the licensor's technology to "talk to" the licensee's particular product. Then a control system and user interface is required, which for a consumer product may be a simple iTunes/Google App. Or for public infrastructure, a more complex network of receivers and control points may be required, together with a software platform or portal by which the end user communicates with the system.

Given the rise in Software as a Service ("**SaaS**") and related technologies, these platforms are often hosted by the licensor (or in the Cloud) and maintained and supported by the Licensor, rather than comprising software which is downloaded and installed locally on the user's servers.

LICENSING OF IoT TECHNOLOGY

The licensing of IoT technology throws up some variations on the usual issues confronting a business when putting in place a technology licence, manufacture or distribution agreement. The added complexity stems largely from the integrated nature of IoT technology, which as can be seen from the introduction above, requires multiple components or services in order to deliver a functional product to the end user. This article is written largely from the perspective of an Australian licensee, manufacturer or distributor. Given that IoT technology is often US based, considerations involving a US licensor also receive some focus in this discussion.

The following sections highlight the issues which, in my recent experience, have proved the more significant or contentious issues in negotiating an IoT licence agreement. There are not a lot of decided cases in the area and it is likely that other issues of significance will emerge as agreements are tested in the courts.

WARRANTIES AND LIABILITY GENERALLY

Putting in place a licence agreement requires careful consideration of who is responsible for what, and who bears liability when something goes wrong. Template licence agreements from US licensors will invariably contain minimal or no warranties, as well as seeking to place the bulk of liability on the licensee.

Anyone who has looked at a few US licence agreements will be familiar with the CAPITAL LETTERS DISCLAIMER OF WARRANTIES, THAT PRODUCTS ARE PROVIDED "AS IS" ETC ETC[4]. This is obviously problematic from a licensee's perspective. While a licensee may be able to procure a limited[5] warranty for any hardware components supplied by the licensor, obtaining warranties for the control platform can be more problematic.

In a recent negotiation the CEO of a US tech licensor told me that, while he was comfortable giving a hardware warranty, "software warranties were hard". This is, in part, because software technology may itself be built on existing standards, eg Bluetooth in the case of wireless technology. The functionality of Apps may depend on smartphone manufacturers such as Apple or Samsung and the corresponding operating systems they allow on their devices. Upgrades to technology by these ultimate providers, the release of new device models and operating systems etc, will themselves have an impact on the functionality which a licensor can provide or guarantee in its control system.

Rather than giving hard and fast warranties, a licensor will generally attempt to approach these issues via the concept of "supporting" their products and services. This may include setting out various "service levels", categorising incidents based on how critical their impact is to the system, and identifying target response and resolution times.

From a legal perspective, such service level agreements ("**SLAs**") can be very rubbery. They generally make no binding promises to fix issues affecting the functioning of the software system, and at best amount to an obligation to "try" to rectify problems. Breach of service levels rarely constitutes a material breach of the licence agreement or entitles the licensee to terminate the agreement.

PERFORMANCE OBLIGATIONS: LICENSEE PROTECTIONS

A licensee in these circumstances should think about trying to negotiate one or more of the following:

- a definitive warranty regarding the functioning of any hardware or software being supplied by a licensor. For example, if a licensor in the course of selling their technology has represented certain particular functionality on which the licensee has relied, the licensee should ask the licensor to stand behind that with a corresponding warranty. Often this can be achieved by incorporating relevant "scope" or "pitch"

documents into the agreement as an annexure. Make sure that any "entire agreement" clause allows for this.

- a positive obligation on the licensor to meet the stated service levels. At best a licensor will usually put their obligation to meet service levels on a "reasonable/best endeavours" basis.

- concrete consequences for breach of support obligations/service levels, which may include credits for falling short of target service levels, or a right of termination or compensation in the event of repeated failures.

- an "Availability" or "Uptime" guarantee for any software control platform. The specifics of this will vary based on the nature of the technology concerned and the licensee's requirements. For example, where the main purpose of the system is to monitor the condition of a device and transmit collected data, it may be sufficient that the system connects to the device and transmits information at least once in a 24 hour period.

  On the other hand, if the devices represent critical components of public infrastructure, for example traffic control systems, any downtime at all for the system is essentially problematic for the licensee.

Other tricks to look for from a licensee's perspective which may affect warranties and corresponding liability on the licensor's part include:

- exclusions for issues caused by "Third Party Software". As mentioned above, the complex and layered nature of software technology means that often particular applications are built on a more general software technology or standard. At a minimum, licensees need to ask the question of licensors what, if any, third party software is involved in the system. If there is, they should ask licensors what contingencies or workarounds they have in place if the underlying software base were to become unavailable for any reason.

- over zealous force majeure clauses which may provide "outs" for licensors, including in the event of data/IT security breaches, supply chain failures, and failure of third party components or systems. When acting for a licensee scrutiny should be given to ensure that such clauses only apply to the extent that such circumstances are not matters falling within the sphere of the licensor's contractual obligations. True "force majeure" circumstances should be genuinely beyond the licensor's control, the licensor having done all things reasonably expected to prevent the relevant circumstances arising[6].

If a licensee cannot negotiate its preferred legal warranty/support position, then the size and reputation of their licensor partner will be important. At the end of the day it is a commercial question for the licensee, but if it has confidence in the licensor's track record of supporting the technology, it may see less risk in practice of accepting a less favourable contractual position.

INDEMNITIES, EXCLUSIONS AND LIMITATION PROVISIONS

Dovetailing with warranties is the issue of who bears liability when there is a failure or defect in the product/service. Given that IoT technology by its nature deals with the operation of physical devices, liability for personal injury and property damage inherently becomes an important risk issue for both parties, far more so than a conventional computer software licensing scenario. Consider the potential risks if a health/body monitoring system were to malfunction, or if your "Smart Home" forgot to turn off your oven or heater at the scheduled time.

Significant factual issues could arise as to causation of a fault in a system which potentially:

1. involves a module (with firmware) supplied by the licensor;

2. the module is inserted into a product manufactured by the licensee;

3. the product utilises a product module interface designed by the parties together;

4. the system is controlled in practice by a (separate) user interface designed and maintained by the licensor; and

5. the entire system is controlled and operated by the end user!

Such factual complexities cannot be solved or avoided in the drafting of a licence agreement, however just getting to a point where each party agrees to bear ultimate liability for those parts of the system which they are supplying can be an arduous process.

Licensors will try to limit their liability on a number of levels, which may involve excluding liability for "consequential" loss, and/or placing a monetary cap on any direct loss suffered by the licensee. This can be problematic in the case of personal injury, where the risk of liability arising may be remote, but the potential quantum of loss very high.

In the case of consumer devices where technology may be relatively simple and sold at a small margin or low per unit cost by the licensor, the licensor may not have "priced in" the risk of personal injury liability as part of their commercial model and may therefore be reluctant to assume any responsibility at all. An overseas licensor in particular may see this risk as something to be taken on by the licensee in its role as the device manufacturer and seller to the end customer.

The licensee/distributor on the other hand knows they will be first "in the firing line" if something goes wrong with a product, especially where the technology licensor is based overseas.

Ideally a licensee would want an unlimited indemnity against loss suffered by the licensee relating to personal injury or property damage, where such loss can be attributed to the licensor's negligence or breach of the agreement (the latter can be harder to get than the former). If that is not possible, licensees ultimately need to assess the level of risk posed by the technology in question, however the following are possible compromise positions:

- excluding only "consequential" and not direct loss; and/or
- raising the overall liability cap in the case of personal injury.

Licensees should also check that their public and product liability insurance will respond to the full range of circumstances which may be foreseeable in an IoT technology system, and that any releases or limitations of liability granted in favour of the licensor do not prejudice the licensee's ability to claim under the policy.

It is advisable for licensees to seek some assurances in this regard from insurers or brokers based on the liability position as set out in the licence agreement.

LEGAL AND REGULATORY COMPLIANCE

Regulatory compliance is another area in which the licensee needs to take some care that they are not signing up for obligations which are beyond their control. For example, in the case of consumer products, a licensor's starting position may be that the licensee should be responsible for any regulatory or compliance issues in the licensee's domestic selling market.

Licensees may be prepared to take responsibility for products which they manufacture, however, the implementation of a consumer product such as a domestic lighting control may depend on a smartphone App maintained by the licensor. End users may in fact register directly with the licensor after downloading the relevant App, thereby entering into an end user licence agreement ("**EULA**") which the licensee is not even a party to and has no control over.

In the case of US based technologies for consumer products this is particularly an issue with respect to privacy law, for example. Australia has an arguably stricter and more unified regime than the US when it comes to collection, management and disclosure of personal information[7]. As often as not in my experience, Australian businesses themselves have non compliant privacy policies, therefore the chances that the generic privacy policies of US based licensors will be compliant with Australian law are not good.

Ultimately the starting point should be, as a general principle, that each party takes responsibility for regulatory compliance with respect to those parts of the system which they have responsibility for delivering.

OWNERSHIP OF NETWORK EQUIPMENT

The application of IoT technology in "Smart Cities" or in industry may require the establishment of a network of data receivers and transmitters, separate to the smart devices themselves, to provide an appropriate data link between those devices and the broader public telecommunications infrastructure. Licence agreements should be clear on who owns such intermediate network equipment, both during and after the term of the licence. The network may need to be upgraded or modified during the term, therefore the licence agreement should address who has the right to request changes to network architecture, in what circumstances, who bears the relevant cost, and what effect changes requested by a party may have on liability issues.

Any arrangement whereby equipment owned by one party forms part of a network operated by another raises issues under the *Personal Property Securities Act* 2009 ("**PPSA**") if the arrangement qualifies as a "PPS Lease"[8]. In those circumstances the equipment owner (usually the licensor) will need to register its interest in order to preserve ownership rights against other secured creditors of the operating party (usually the licensee).

To assist in that regard a licensor will want some general provisions in the licence agreement regarding the cooperation of the licensee with registrations, and the waiver of some of the procedural aspects of the PPSA. Similar considerations would arise for the licensee with respect to their end customers if the licensee is the owner of network equipment which passes into the customer's possession.

SUMMARY

As with any technology licensing arrangement, there is a range of other issues which will need to be considered in an IoT licence, including exclusivity, sublicensing rights,

IP ownership, testing & acceptance procedures, FX provisions, as well as breach and termination. These and other issues will be addressed in detail in Part Two of this article.

While the legal complexities may seem daunting, clients who address the issues raised in this article in an organised but commercial manner will give themselves the best chance of success when embarking on an Internet of Things project.

FOR MORE INFORMATION, PLEASE CONTACT:

PETER KARCHER //
Partner

T 61 2 8235 1218

E p.karcher@clarkekann.com.au

[1] *That "Internet of Things" Thing,* Kevin Ashton, RIFD Journal, 22 June 2009: http://www.rfidjournal.com/articles/view?4986

[2] Some good examples of IoT technology are provided at: http://postscapes.com/internet-of-things-examples/

[3] See *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*, Gartner, 10 November 2015: http://www.gartner.com/newsroom/id/3165317 and *The Internet of Things: How the Next Evolution of the Internet is Changing Everything,* Dave Evans, Cisco, April 2011: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[4] This can actually work to a licensee's advantage if the licensor's local lawyers have not inserted an exception for non excludable warranties under the *Competition and Consumer Act* 2010 and taken advantage of the permitted limitations to resupply of the goods/services concerned, or paying the costs of having the goods/services resupplied – refer *Australian Consumer Law* Part 3-2, Division 1, esp. ss 64, 64A, although note these provisions only apply to certain types of transactions and may not apply depending on the circumstances.

[5] In the sense of the warranty being limited as to time, and often limited to "defects" rather than a warranty as to particular functionality.

[6] For example, a licensor should not be entitled to rely on a purported "force majeure" clause that includes "virus/security breach" in circumstances where the licensor has failed to maintain appropriate data security measures.

[7] See for example *Which countries are better at protecting privacy*, by Constance Gurke, BBC Capital, 26 June 2013: http://www.bbc.com/capital/story/20130625-your-private-data-is-showing.

[8] *Personal Properties Securities Act* 2009 section 13.