Presentation on Intellectual Property Issues
For the Internet of Things: Key Legal Considerations

Autonomous vehicles:
a stalking horse for intellectual property rights for The Internet of Things

By Richard C. Balough[1]

Thanks to the previous speaker, you have a brief description of what the Internet of Things (IoT) is. Now I want to explore with you one example of the IoT that you may deal with every day to help understand intellectual property issues as they relate to the IoT.

You have heard about the coming of driverless cars or autonomous vehicles. They are a good example of the IoT. They are machines connected to and exchanging data on the internet and taking action without human intervention.

A bit of car evolution is in order. From the beginning, cars were self-contained machines. While they had had electrical parts, and eventually some computing ability, these early systems were not connected to the outside world. This is sometimes referred to as air gapped, which by the way, was the practice for many industries. Access to the car’s computer systems was made via a OMB II port when the dealer manually connected to it. Of course, once connected to the car’s systems, all systems were vulnerable because there was no thought of outside intervention and thus, no need to protect the systems from the outside world. There were no software or hardware firewalls because no one considered the implications of being connected to the outside world or the internet.

As cars became more complex with entertainment systems, GPS, tire pressure gauges, and other conveniences, they became computers on wheels. With Bluetooth and Wi-Fi, cars no longer are isolated vehicles but rather are connected to the internet. As cars become semi-autonomous—think lane change warnings, auto pilot, collision avoidance—the systems gather data from outside source such as the internet to take action.

Today there are four driverless Ford Fusions on the road in Pittsburg being tested by Uber (actually there is a standby driver and engineer in the front seat). A driverless car is a manifestation of the internet of things. Driverless cars communicate via Wi-Fi and the Internet with other vehicles and systems. In other words, cars are one aspect of the internet of things—machines interfacing with and affecting other machines without human intervention.

So what does this all mean, especially to business lawyers? Well, first of all, cars are just one example. But since we are all familiar with them, they are a good vehicle, so to speak, to talk about intellectual property and the internet of things.

[1] Richard C. Balough is a founding member of Balough Law Offices, LLC, a Chicago, IL. Based law firm that counsels small to medium size closely held entities in protecting their intellectual property, especially in cyberspace. He is a co-chair of the American Bar Association’s Mobile and Connected Devices subcommittee of the Cyberspace Law Committee.

As with many IoT applications, there are three basic elements that need intellectual property protection.

First, the actual device or chip or combinations. In many IoT applications, the actual device or chips may be far from view or not readily apparent. Second, there is the code that drives the device and connects to the internet and other machines or devices. Third, there is the data itself.

Let’s take a more detailed look at each.

The hardware. From a legal perspective, there is nothing extraordinary about the hardware. If the hardware is new and useful, novel, and non-obvious, it may be patentable. Not being a patent attorney, I will leave it at that. The hardware may also be protected as a trade secret. Admittedly, this would be a difficult row to hoe. If the hardware is out in the public, how do you prove that you have taken reasonable measures under the circumstances to keep it confidential and gain economic value from keeping it from others?

So for business lawyers, here’s my suggestion to you regarding your client’s hardware: ask your client: Is what you are developing for the internet of things, new, useful, and non-obvious? Maybe there is a possibility for a patent. On the other hand, is what your client is developing infringing on an existing patent? If neither of those is true, is the device a “black box” that may be protectable as a trade secret for what goes on inside it?

The code. Here is the heart of intellectual property for the internet of things. Protecting the code can be done in several ways. If it is original code, it may be copyrightable. If it is copyrighted, then the owner may also prevent access to the code by implementing anti-circumvention protections. Under the Digital Millennium Copyright Act (DMCA), it is illegal to circumvent anti-circumvention measures to access copyrighted materials.

Let’s go back to my car example. You say, this is my car. I bought it (or lease it), so why can’t I have access to the code that operates it? If I want to customize the software to make the car go faster or pass emission tests when the car is hooked up to the tester, why can’t I? Doesn’t the “first sale” doctrine apply? Hey, isn’t it fair use for me to work on my own car?

Well, did you actually buy the software in your car or did you merely license it as you do most software? Have you read your end user license agreement (EULA?)

And then there is the DMCA anti-circumvention provision. If you by-pass a car’s anti-circumvention protections, absent an exemption, you may be violating the DMCA. A year ago, the U.S. Copyright Office, over the objections of car manufacturers, granted two exemptions where circumvention would be fair use when accessing a car’s code.

The first exemption allows an “authorized owner” to diagnose, repair, or “lawfully” modify the code as long as it does not violate other statutes. This exemption retains the ability of car owners to work on their own vehicles as long as they do not make modifications that would disable or downgrade pollution control systems in violation of the Environmental Protection Act. However, the exemption does not apply to computer programs chiefly designed to operate a vehicle's entertainment and telematics systems.

The second exemption permits security research "for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, when such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public." The exemption was opposed by car manufactures who claimed that the security research could be used by "bad actors" to hack into cars.

So for a business lawyer, what is the take-away? If your client is developing original code, you may want to consider copyright protection. And if possible, you want to include anti-circumvention methods to protect the code. You also want to have, if possible, a EULA that limited the right to use the code and prevent unauthorized copying. If, on the other hand, your client wants access to code, what are the contractual restrictions? Has the owner put anti-circumvention measures in place? Is your client's use a fair use or is there an exemption from the DMCA for the use?

But we're not done with copyrights. So far we have discussed original code created by your client. However, a lot of code driving the internet of things is not all original code. Many developers use open source code. You need to know that open source code does not mean it is free code that a developer can use in any way he or she wants and then charge others for the code. Open source code is licensed with restrictions as to its use and incorporation into other code. Depending on which open source agreement the code is licensed, different use restrictions apply. Generally using open source code means changes will need to be open to the public for others to use.

For example, under the GNU Lesser Public License all versions of a program remain as free software for all users to use and modify. Section 3 of the license (Version 3) provides that anyone using a "covered work" cannot forbid someone from accessing the source code when the program is conveyed. A "covered work" is either an unmodified program or a work based on a licensed program. "Convey" means "any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network with no transfer of a copy is not conveying." If the software is incorporated into a program that does not enable "other parties to make or receive copies," then its use does not "convey" the software under the license and would not trigger the requirement to disclose or provide access to the modified software.

So, you need to talk with your clients to understand what open source code they may be including in their IoT application and read the license to determine if they then must disclose their changes to the public.

In some circumstances, the code driving the IoT application may be embedded into the chip or device with only the executable file made available. In this circumstance, it may be possible to preserve the source code as a trade secret.

The data. If code and software are the heart of intellectual property protection for the internet of things, then data is the payoff. Data is intellectual property that includes not only the method by which the data is obtained but also what the data discloses, which can be monetized.

But before it can be monetized, there is the fundamental question of who owns the data? If I drive my car, or in the case of a self-driving car, it drives me, who owns all of the data generated? The data includes when I drove, where I drove, how fast I was driving, how aggressive I was in my driving. This is great information for an insurance company to set my rate. It may be great information for health insurance rates. If I pass by a certain store every day, then wouldn't they like to send me a push notification on a sale? These questions also have privacy implications. Proper disclosure of what is being collected and how the information is being used may create legal concerns, which other panelists will discuss.

So here's my take-away on intellectual property regarding data. Make sure your client knows who owns the data. If your client is collecting data, make sure the client complies with all regulations regarding the collection of data and lets the person whose data is being collected know what is being collected and what is being done with the data.

Finally, I want to have you look to the future. As the Internet of Things develops with machines talking to machines, those machines will be developing their own intellectual property. So who owns the patent or copyright of a product or code generated by a machine?

Well, maybe a monkey can help answer the question. If you don't know a monkey, a monkey who took a selfie and the image became famous. A photographer who owned the equipment sold the images but the monkey sued saying he owned the copyright because he was the "author" for copyright purposes. The monkey lost and the US Copyright Office issued an amended compendium of its office practices to state that "to qualify as a work of authorship a work must be created by a human being." Listed as examples were a photograph taken by a monkey and a mural painted by an elephant. More importantly for our discussion, the compendium also said: "Similarly, the Office will not register works produced by a machine or mere mechanical process that operates randomly or automatically without any crated input or intervention from a human author." So then, who will own the works when machines are the creators?

If all of this intrigues you, then I invite you to attend the ABA's Cyberspace Law Institute on January 20-21 in San Diego.