Intellectual Property Consideration for the Internet of Things

What is the Internet of Things (IoT)?

The Internet of Things ("IoT") is the network of devices embedded with sensors, actuators, electronics, and software enabling these objects to exchange data. Think of IoT as connecting any "thing" with an on/off switch to the Internet.

But IoT extends beyond connectivity to encompass distributed computing, enabling devices to store data, coordinate with each other, analyze data, and make decisions on their own. Just as the smartphone has brought immense changes to the conduct of our personal lives, IoT brings the promise of new efficiencies to virtually every "thing." Consumer products, factories, logistics, electronic commerce, building management, smart homes, security systems, patient care, health monitoring, power grids, autonomous vehicles, and urban planning are just some of the places IoT has already found use.

What are the IP risks for a new entrant?

The technologies enabling IoT include sensors and actuators, wired and wireless networking, computing and storage, analytics, user interfaces, and services. The Intellectual Property (IP) landscape for these diverse areas differ in scope and maturity. Sensors and actuators tend to be older, analytics and services tend to be newer, and the in-between technologies, such as connectivity and computing, tend to leverage features found in prior Internet applications.

Many established players already own significant intellectual property (IP) in one or more of these spaces. Before going to market with a newly planned product or service, it is wise to consider where the possible infringement risks lie.

Are you planning to purchase a large part of your solution? Structure strong indemnity clauses in the contracts with your suppliers.

Or do you plan to design your own solution? If so, assess your freedom to operate. Seek licenses or have a good non-infringement or invalidity defense ready, especially in the "in between" areas where there is a dominance of mature companies and patents.

How Can You Establish Your Own IP Rights in the IoT Space?

That is not to say that all of IoT is merely the repurposing of old technologies to new uses. A clever or aesthetic design for a connected consumer device, improved analytics for a particular application, or a specialized interface are but some of the places to establish an IP beachhead.

More generally, the IoT industry still desperately needs improved ways to certify and control the connected things and to ensure the network is secure. Standards organizations such as the IEEE, NIST, Open Connectivity Foundation, and others are working in these areas. There may be opportunities to establish essential IP beneficial to others by coordinating with these groups.

What IP Legal Challenges are Specific to IoT?

IoT presents a combination of challenges to the IP strategist that are not unlike other computer-related technologies.

Because IoT involves devices interacting with each other using an ecosystem that spans from connectivity to distributed computing and analytics, it is far too easy to draft a patent claim that will never be enforceable because it is only infringed when multiple parties act. Recent court decisions such as the Supreme Court's *Akamai* line of cases have clarified the law of divided infringement, and liability can be found even when multiple actors are involved. But it is best to start by carefully writing patent claims so that they only require a single actor to perform all steps.

The law of patent-eligible subject matter also continues to evolve. The Supreme Court's *Alice* decision has clarified that merely implementing an "abstract idea" on a computer will not be eligible. On the other hand, an invention that involves control over a physical thing, provides an improvement to an existing technology, or is not merely a routine and conventional solution to a known problem, is not "abstract" and will be eligible for patenting.

If your novel implementation tends more towards specialized analytics, or the software logic underlying a service, it may be best to keep the details of that confidential. Rely instead on copyright as well as the Federal protection now afforded by the Defend Trade Secrets Act.