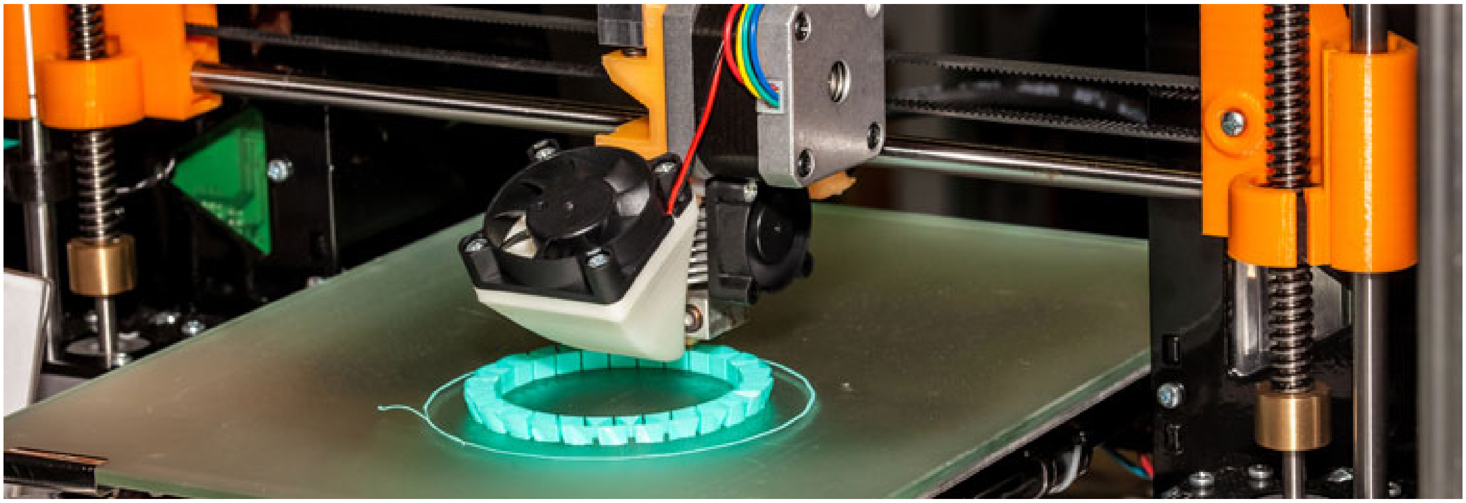
DLA PIPER



Industry 4.0. The Fourth Industrial Revolution. The Industrial IoT. IIoT. What are they anyway?

13 MAR 2018

By: Luke Stubbs LLB

They are different names for what is essentially the same thing − the adoption of new advanced technology and systems by industrial and manufacturing businesses − with a particular emphasis on connectivity.

This adoption could happen at potentially any point in the value chain: from automated purchase and ordering of materials and components (based on intelligent resource planning systems and even end-customer sales data), smart route and delivery planning, management of inventory, smart design of products, automated production lines (with sensor enabled monitoring), 3-D printing and additive manufacturing, through to diagnostics (giving insights into efficiency and flagging potential plant failures and maintenance needs).

More widely we are entering the era of smart power grids, connected factories, smart cities, autonomous vehicles and so on.

Common themes are machines and systems which are "smarter," increased AI and automation, use of sensors to capture and share more data and information, and everything being connected through the cloud.

So what are the legal considerations if I am looking to buy this technology?

Well, we're glad you asked!

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as

Deal or no deal

You will still need a contract with the suppliers of this new technology. They may even be your existing suppliers who have developed new products and systems.

However, when you drill down, some key questions arise:

- What terms is my supplier proposing? Will I have to agree to their standard terms? Are they looking to supply under an existing contract or a new one?
- Does the proposed contract cover all of the key risks? Does it adequately address potentially new issues, like who owns the data which is produced or how the data is protected?
- Am I buying a "product" or a "service"? Who is responsible for integrating the various parts of the new system?
- I used to buy maintenance separately − can I still do that?
- What liability is the supplier accepting or excluding? I am relying on this new system to deliver a significant saving − can I recover that if there is an issue? Where do I stand if a machine makes a bad decision?
- What assurances am I going to get about performance, and what are my remedies if something goes wrong?
- When we procured our network connectivity, we didn’t expect to be using it to run our factory. How will this new contract fit with my existing ones with other suppliers?

But is it legal?

Advances in business and technology bring new challenges to ensure compliance with regulation (much of it written before the technology was invented). Whether it is compliance with health and safety or equality and anti-discrimination laws, numerous rules will need to be navigated when introducing new ways of doing things.

For example, a system that allocates workers to roles based on their physical abilities may make perfect sense to a machine, but it could potentially put their employer in breach of anti-discrimination laws which require more human value-based decisions. Elsewhere, a system which sets shift patterns to maximise efficiency or use cheaper power will need to fit with working time legislation.

It will be important to understand how a system will be used, what it will be doing and what rules and regulations could apply. Some of this may need to be reflected in a system's specification or the warranties that the supplier is giving.

Hey, that was my idea!

Suppliers have always sought to protect and defend their valuable IP, first in the design of machines and more recently in the code which runs them.

IIoT and its associated technologies greatly expand the types of IP which may be relevant. Industrial designs, patents, copyright, semi-conductor topography rights (yes, that is a thing) and database rights, to name a few, could all be involved.

Because it is difficult to protect and patent processes, or patent software, there is also still an important role for more intangible forms of IP, such as trade secrets, confidential information and know-how (which are normally only protected via practical steps and contract obligations).

As IP becomes more prevalent, some key questions arise:

- What IP do I own or use and what will I need to share with my supplier? How can I protect that?
- Of the IP I use, does any come from a third party? Am I allowed to share it with third parties, including my suppliers, without infringing?
- If my supplier (or a system it provides) creates some new IP, such as images, important data or even improvements to my own processes or products, who owns that?
- If I commission a supplier to create a system which will give me an advantage over the competition, can I ensure that the supplier keeps it a secret and does not productise it?

Knowledge is power

You may already be familiar with concepts such as big data, data mining and analytics. Retailers and banks have been talking about them for at least a decade.

They are a key benefit of automation and digitisation. The more sensors and systems that monitor what is going on, the more data is created. Aside from the IP considerations above, that data can be very valuable to a business in understanding how its processes run, where it is doing things well and what can be improved.

If you are a supplier, that information can tell you how your customers use your product, how that product fits with their environment and what improvements could be made. It can show when maintenance is needed or if a breakdown is looming. It could also give you broader information, such as how the wider business is doing or how a company runs its plant.

And there it is. One of the key prizes for the suppliers of all things digital and automated to their industrial customers is insight. OEMs who once provided equipment, maybe some control software, and extended warranty and support visits can now provide "servitised" systems connected to their control centres. They can schedule maintenance visits or repairs before a problem happens. They can anticipate which products or services may add real value to their manufacturer customers and start to develop them. They can understand their customer's operations and how they do what they do. Most importantly, they can potentially see that for all of their customers. The value attributed to this sort of data cannot be understated. It has been described as the new oil.

A deep understanding of its customers has potentially huge benefits for the supplier and ultimately the customer, but there are some key considerations for example:

- Who "owns" the data which an IIoT supplier creates about my business?
- Can I control how it is used?
- How do I ensure that it is kept secure and what happens if data about my business is given to a competitor or is stolen.
- What obligations can I impose to ensure that the data is still available if the supplier's infrastructure breaks down.
- On termination of my supply agreement, how easily can I move relevant data to a replacement supplier who will provide the same service but using a different system? Will the data be compatible?

This time, it’s personal

You may be familiar with the new General Data Protection Regulation, which will come into full force in the UK in May 2018. If not, where have you been!? The GDPR represents the biggest overhaul of data protection law in two decades, and introduces some important new concepts such as privacy by design, direct regulatory responsibility of service providers who process data for others, obligations to report data breaches to regulators within 72 hours, and potentially huge fines for non-compliance (up to €20 million or 4 percent of global turnover).

As well as all of that, it will also widen the definition of what actually counts as "personal data,− so much so that it will arguably include, for example, the IDs and location information of factory workers or drivers who may have to log into a smart system used by their employer.

The point is that with more and more personal data being produced and handled by ever-improving systems, the need to ensure compliance with a more comprehensive than ever data protection regime comes to the fore. To do that, a business will need to have considered its operations, how and where it will create and use data, where that data goes in its supply chain, what policies and notifications it has in place, and upon what terms (including in relation to compliance and liability) its suppliers are willing to handle that data.

Final thoughts

These are exciting times. Advancements in technology are revolutionising how we live and work. In industry, the potential efficiencies and savings from adoption of new technology go beyond the wildest dreams of every Six Sigma Blackbelt. Digital is the new Lean.

The UK government also wants to encourage growth and adoption. New technology and the productivity benefits which it can bring are a focus of the UK's new Industrial Strategy. Led by Siemens' Juergen Maier, the Made

Smarter review is a key part of that, and explored how UK manufacturing can maximise benefits from increasing adoption of digital technology.

Overall, the signs are positive, and to compete post-Brexit and on a global stage, UK manufacturers will need to be as efficient and effective as possible.

In legal terms, yes, there are issues to consider, and risks which may need to assessed and managed.

However, they should not be seen as a blocker to innovation if they are carefully considered. After all, that is what lawyers are for (until we're replaced by machines).

About the Author

Luke Stubbs is a Legal Director based in DLA Piper UK's Manchester Office. He is a member of the IP and Technology Team, and leads our Manufacturing Sector group in the North West UK.

AUTHORS

Luke Stubbs LLB
Legal Director
Manchester | T: +44 (0)20 7349 0296
[email protected]