Roundtable: interoperability and data ownership in the IoT

E-Commerce Law & Policy explores the data ownership and interoperability issues applicable to the Internet of Things ('IoT'), with contributions from four experts.

Realising the future

The IoT's future potential is enormous for an increasingly connected world and a smarter technology infrastructure to power our lives. However, to realise that future, there are some important middle steps to get there. Central to that is the question of data ownership. So much data is, and will be, produced by these connected 'things' but there is ambiguity as to who owns that data. This is a vital discussion that impacts business models, law, policies and governance.

The early stages of IoT are interesting: smart meters to help improve energy efficiency and wearable technologies tied to analytics to improve personal health, are compelling applications. What happens when there are tens of billions of connected devices such as sensors embedded in cars, infrastructure, etc.? Who owns this data? The individual, the product manufacturer, the service provider? Where is that data stored, and who has access to it? These questions around data ownership have far-reaching implications, from security to privacy as well as legal ramifications. There has been some early progress on this front. The US National Telecommunications and Information Administration has recently issued a Request for Comment on how issues raised by big data impact the Consumer Privacy Bill of Rights. The focus is to put individuals in control of their own data and how it is used and safeguarded.

Understanding who is the steward of data is important (regardless of data ownership). In addition, how will data be accessed? Portal-based, via API-calls, or other access mechanisms impact both infrastructure and data usability. Likewise, how the data is defined and the drivers behind those definitions need to be clarified to ensure accessibility and utility of the data. Security is also vital, and must combine both effective policy and strong execution. Lastly, who owns the derivative information about the data? The models and data produced in the future can create a wealth of opportunity around powerful analyses and lucrative financial benefits as IoT data and models of the future evolve. It's hard to pin specific examples down, but setting the tone in the early stages of IoT maturation around ownership of derivative data is important to plan for as this area matures.

This is a global shift that is happening, a path to an increasingly connected world that is both exciting and complex. The global implications are just as important to get correct as the local implications. It's going to take participation and involvement by a number of stakeholders. While device, product and application manufacturers will have a voice, consumers should ultimately have control of their IoT data. Governments and policy makers should serve a role that forces the issue of data protection, and technologists and futurists should help shape the industry dialogue to shepherd us to the connected future that can tap into the IoT without sacrificing privacy or security.

Nikki Gore Vice President of Marketing
Infobright, an analytic database platform provider serving as a key infrastructure for the IoT
Contact via Matt Flanagan at matt@famapr.com

Ownership disputes ahead

We can expect to see big disputes about who owns the data generated in the IoT. There is no property right in data themselves. The owner of a smart thermostat, for example, does not own the usage data it generates. The only thing that is 'ownable' is an organised aggregation of data which satisfies the statutory definition of a 'database.' Database right is an EU-specific IP right that is designed to incentivise and protect the storage of data.

Ownership of databases can be established by contracts between the appropriate people and that is the clearest way to do so. Where a contract does not exist, the general law will determine who owns what. But the nature of the IoT means that it is often very difficult to identify satisfactorily who in a chain of data, from user to the ultimate store of the data, owns the aggregation of data.

The first owner of a database right is its 'maker.' The maker is defined as the person or organisation that takes the initiative in obtaining, verifying or presenting the contents of the database and assumes the risk of investing in that process. It is the maker who therefore controls the ownership of the database. This requires an assessment of who is doing what in the process and who is ultimately economically and commercially responsible for it happening. Whoever physically collects or presents may not be the 'maker,' particularly where this process has been outsourced to a third party service provider. More than one entity may take the initiative or assume the risk and, if so, they will jointly own the database right.

Given the overlapping responsibilities and roles of those in the data chain, it is vital to put in place appropriate ownership

provisions in the relevant agreements.

Adam Rendle Senior Associate
Taylor Wessing, London
a.rendle@taylorwessing.com

The interoperability challenge

In a world where technology is becoming ubiquitous, the capacity to exchange and share information autonomously between people, between objects and between people and objects within a specific context is a fundamental issue. We not only want all these network-connected applications to be able to exchange and share information, but also use this information to make decisions and in doing so make our environment intelligent.

The ability to seamlessly exchange and share information between for instance people, smartphones, wearables, sensors and actuators in their environment is also referred to as interoperability of information, which can be defined as: 'the realization of mutual connections between two or more systems or entities, to enable systems and entities to exchange and share information in order to further act, function and produce on the principles of that information.'[1]

In a positioning paper written by the IoT Special Interest Group in the UK[2], the possibility of being able to share and exchange information between actors in networks such as the IoT is seen as the biggest challenge. The problem of interoperability of information within sectors is already big, but it is even more complex when information has to be shared and exchanged across sector boundaries. According to the Special Interest Group, the problem of being able to share and exchange information within and between sectors is too often approached from a standardisation point of view.

There is no property right in data themselves. The owner of a smart thermostat, for example, does not own the usage data it generates

The Special Interest Group notes that the challenge of being able to share and exchange information in order to develop this kind of new and intelligent environment requires a different approach. In its view the new approach has to be based on the development and shaping of international interoperability frameworks that simultaneously serve as design guidelines and best practices within the evolving global network of the IoT.

Ben van Lier Director of Strategy & Innovation
Centric, a software solutions, outsourcing and staffing services company
Ben.van.Lier@centric.eu

1. Lier van B. (2013): 'Can Machines Communicate? The Internet of Things and Interoperability of Information.' Engineering Management Research, vol. 2, no 1, pp. 55-66.
2. 'Internet of Things and machine to machine Communications (M2M): Challenges and opportunities' – final positioning paper – May 2013. IoT Special Interest group. Technology Strategy Board.

Future interoperability

Interoperability refers to the compatibility of computers and networks in all possible respects. Thereby, a central IoT issue concerns the problem of establishing future interoperability: the IoT may be used in ways that are hardly foreseeable at this moment. Furthermore, the design of the internet being subject to changes influences the functioning of the IoT. Looking at the very complex fast-developing technologies, the challenge exists that adaptations in either the internet or the IoT will always have to be communicated to the other system and the respective changes will have to be installed. Such a mechanism is likely to be labour intensive and require a high degree of information exchange.

Interoperability of different parts of the IoT requires a certain degree of standardisation. Incentives for standardisation are low if the respective transaction costs of its development swamp the benefits; in addition, standardisation can eliminate competitive advantages and collide with antitrust law.

Interoperability also requires that providers of software are able to manufacture products that operate with other systems and programs, making it necessary to exchange interface information, i.e. information about systems and programs of other producers, which may be protected by copyright. If the market is dominated by one provider antitrust law questions related to the existence of a dominant undertaking are at stake: If the provider can demonstrate that the supply of information is indispensable to carry on its business in the market, and the refusal of this supply results in a risk of elimination of competition, which may in turn impact technical development to the prejudice of users, the dominant provider may be forced to supply the necessary information (the so-called essential facility doctrine).

An approach to an adequate interoperability of the IoT could consist of a separation of its functionality from its technical implementation, i.e. in an integration of a diverse set of technologies into the structure of the IoT. Such an approach allows for the application of different solutions to different applications. Furthermore, an infrastructure including various technologies is future-proof, as an infrastructure built with heterogeneity in mind will easily implement newly developed devices and networks.

Rolf H. Weber Chair Professor of Law
University of Zürich
rolf.weber@rwi.uzh.ch