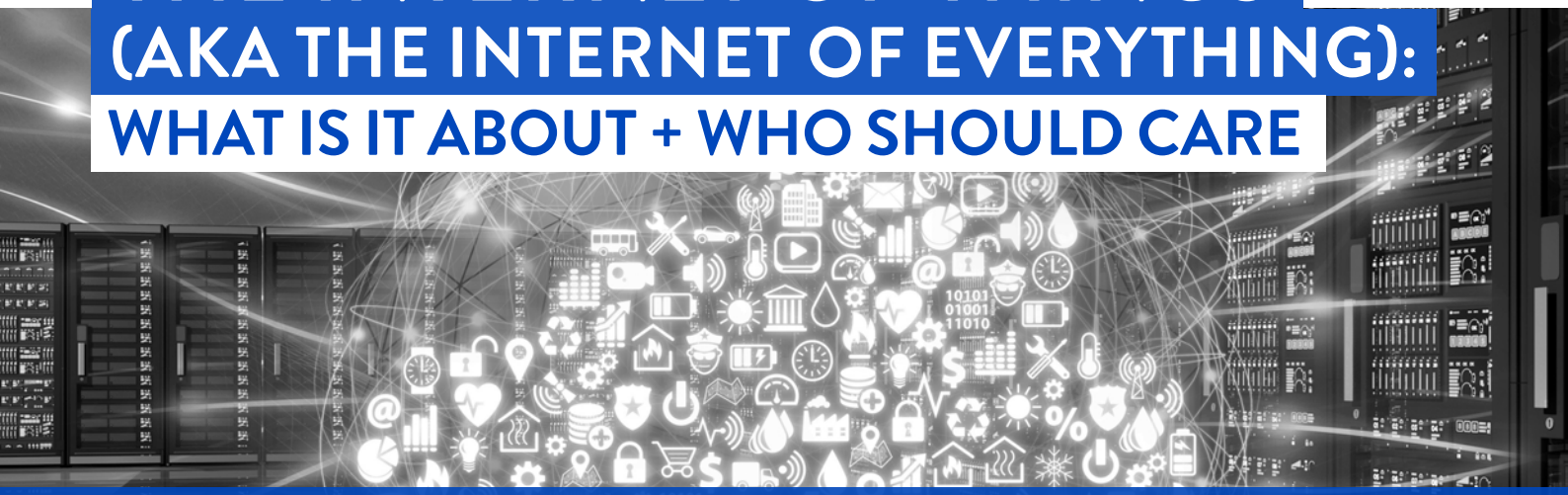
GILBERT +TOBIN

# THE INTERNET OF THINGS (AKA THE INTERNET OF EVERYTHING): WHAT IS IT ABOUT + WHO SHOULD CARE



PETER G LEONARD, PARTNER, GILBERT + TOBIN LAWYERS

**Data is at the heart of the Internet of Things (or IoT, also known as the Internet of Everything).**

**Management of data handling and data analysis, and of data sharing between business entities, will be a core issue in provision of most IoT services. Data management is also critical in the operation of IoT communications platforms and the sensor, communication, control and reporting devices used in IoT services. Diverse data capture, multiple data flows and substantial value-add by data analytics are at the essence of IoT services.**

AUGUST 2016

More and better data creates significant opportunities for most businesses. It also brings disruption to many existing business and new sources of business risk.

This brief paper outlines opportunities and risks.

At its most basic, the IoT is the concept of connecting any device with an 'on' and 'off' switch to the Internet and/or to other devices. IoT devices may be any device capable of connection: hence the alternative moniker for the IoT of *the Internet of Everything*.

IoT devices include everything from vehicles, smartphones, thermostats, kettles, swimming pools, washing machines, headphones, lamps, wearable devices and so on. The IoT also refers to remote monitoring of components of machines, such as a jet engine of an airplane or an electricity network, and remote operation of machines, such as mining vehicles or undersea craft.

A key element of many IoT services is the incorporation of sensor devices. These sensors may either be passive devices that monitor and report over the Internet as to conditions in a particular environment, or active (actuator) devices that change conditions in that environment.

Frequently an IoT service will be machine-to-machine, rather than human-to-machine. Absence of direct human intervention may lead to concerns as to awareness of affected individuals in relation to ongoing collection and handling of personal information about them in the course of provision of such services. Some IoT consumer applications provide consumers with information that enables them to make actionable decisions based upon the analysed information (for example, 'smart home' applications to turn on an air-conditioner, to turn off a pool filter or to order chemicals required to treat a swimming pool). Other applications may fully control and self-adjust in response to a particular environment without any active consumer intervention (for example, smart

home applications that respond to an extreme weather event by automatically activating sprinklers, closing curtains, turning off non-essential electrical appliances and turning on an air-conditioner that services a pet area).

IoT has been much hyped. IoT is probably near the peak of the now familiar technology hype cycle. That noted, a report released by Macquarie Equities in July 2016 and entitled *I Robot, Who can win from digital disruption*, identifies "four mega trends" that have the largest potential to disrupt the Australian corporate landscape over the next decade, being virtual reality, wearables, big data and IoT. Cisco Systems estimates that IoT will increase US corporate profits by 21 per cent in the next eight years, derived through reduced costs from higher asset utilisation, higher labour productivity, lower waste and improved supply chain logistics, new customers from improved product experiences and reducing the time to market for innovations. Macquarie Equities also suggests that due to the increasingly rapid business impact of technological change, the opportunity cost of businesses being slow to adopt technologies will rise exponentially.

There is no doubt that technological factors are converging to escalate the pace of IoT deployment. These factors include:

+ as to sensors, rapid reductions in cost consumption coupled with improvements in capacity, durability, robustness and power efficiency
+ improvements in communications technologies between sensors and hubs and control devices, including 'meshed networks' and other improvements in bandwidth utilisation and reliability
+ improvements in encryption and other technologies to protect security of data both at rest and in transit
+ rapid uptake of smartphones, enabling near ubiquity of availability (subject to mobile network and wi-fi coverage) of a relatively low cost and globally standardised device which enables insights to be delivered to users and the smartphone used as an actuator device
+ rollout of cloud based data warehouses and cloud based analytics platform services, enabling interconnectivity of services and low cost set-up and tear-down of data sources and analytics capabilities
+ rollout of broadband and narrowband networks and IoT platforms and hub devices that support third party IoT services - many low cost IoT smart home applications require access to an IoT hub device, such as a Nest device, provisioned by a third party such as a consumer.

The opportunities afforded by IoT come with attendant risks and challenges, many novel and requiring development of new business models, law and new forms of contract.

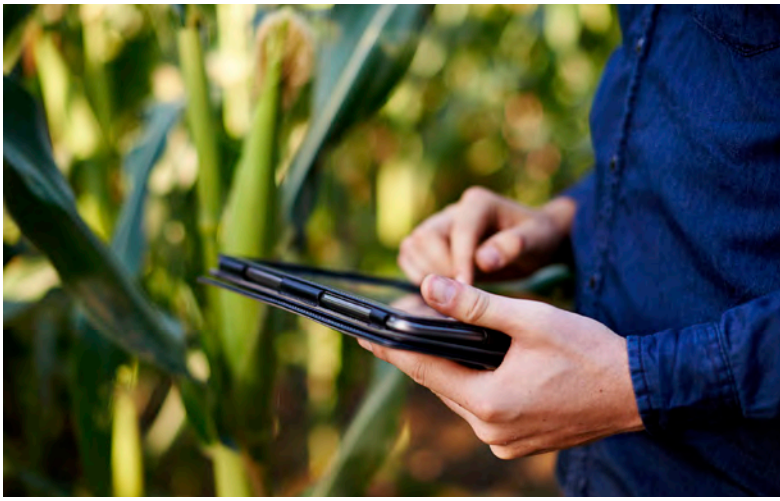
Often third party supplied devices will be integral to the service delivery chain. For example, a smart home application may communicate with service providers by means of the Nest platform as bought and installed by the consumer and with the householder by an app on the householder's smartphone or tablet. The variety of device and service options may lead to issues as to responsibility for malfunction in provision of a service caused by failure of third party supplied devices or communications platforms and carriage services.

Data errors or omissions or breakdowns may also lead to incorrect decisions being made in reliance upon data analysis that is correctly carried out but using data that is adversely affected by data errors or outages. Because sensoring may rely upon proper operation of third party devices and some operating issues will not be capable of remote detection, the reliability of IoT services may be adversely affected by data quality issues of which the IoT service provider is unaware, even if the IoT service provider exercises all reasonable diligence in real-time monitoring of service quality.

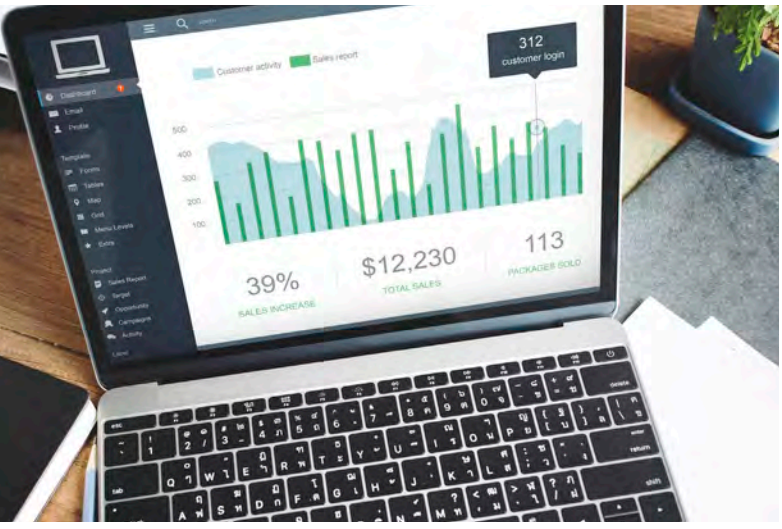
Clearly, data quality is important to ensure that IoT services provided using such data are reliable and accurate. Many IoT applications will draw upon one or more external data sources to bring together various data inputs for analysis and outputs that either autonomously make an actuating decision or that present a dashboard of analysed information that enables a human user to make an actionable decision. Making data available for diverse applications creates legitimate concerns as to the legal liability for data sources, including public sector entities, that capture, curate or make available that data. Many data sources will be concerned that raw data may be incomplete, intermittently available or otherwise unreliable and accordingly unwilling to release that data without quality assurance.

Particular concerns arise where data may be used in applications that are beyond the contemplation of the data source: for example, where meteorological predictions are used to make machine-driven decisions as to climate control in factory farms.


Similarly, providers of IoT communications platforms may be concerned that these platforms may be used for high availability, high risk exposure applications of which they are unaware. Concern as to legal exposure may impede government agencies or businesses from making decisions to release data for potential uses that are not controlled or managed by the data source. Concern as to exposure that may arise through data capture and availability may also impede prospective users of IoT services from making available their data for use in those services. For example, a farmer may be concerned as to prospective use by environmental activists or environmental regulators of on-farm data that the farmer contributes to an IoT service, or by commodity brokers or traders to gain an informational advantage in price negotiations with the farmer.



Concerns as to data quality and potential legal liability arising out of reliance by IoT service providers or end users upon that data are particularly likely to further impede release of data sets by government agencies. Many governments around the world have stated their commitment to the release of public data wherever practicable, implementing policy that public data should be a public good. However, open government data will be impeded unless liability exposures as may arise from data quality issues, or reliance by users, are appropriately assessed and mitigated. Many applications of government data may not be anticipated by the government agency that captures, curates or makes available that data. Uses often involve creative combination and comparison of multiple data sources by a data user that creates and manages an IoT service. Consider an agricultural IoT service that enables a farmer to make actionable decisions by means of a 'dashboard' report that provides analysed data outputs ('insights') on the farmer's smartphone. This service may combine data from field sensors measuring moisture content in soil and on plants, meteorological data provided by the Bureau of Meteorology, soil maps and river hydrological data from State agriculture agencies, and on-fram soil analyses by agronomy service providers, all mapped onto geo-spatial maps that combine public sector licensed geo-spatial data with third party corporate value-adds which enable annotations and other value-added features and functions. Failures or other errors in any of these data sets may compromise the information base and quality of analysed data outputs.




Providers will also need to consider the impact of privacy laws. Where activities of persons with access to data about individuals are not appropriately controlled through deployment of reliable contractual, operational and technical safeguards, release of data that has been de-identified but not fully anonymised (and which therefore remains vulnerable to concerted re-identification attack through combination of the data with other data) may lead to individuals becoming reasonably identifiable. In such cases, any disclosure of this de-identified information could be classed as a release of personal information.

For businesses, there are additional risks. Many of these risks relate to a fundamental issue, being that currently in Australia and many other jurisdictions legal recognition and protection of proprietary rights in data are somewhat uncertain and may not be fully effective to enable appropriate control over downstream uses of data. More specifically, developing equitable doctrines as to protection of trade secrets or confidential information may not be adequate to protect sharing of 'commercial-in-confidence' data as required for many IoT services, particularly where an IoT service provider is not vertically integrated and relies upon other entities to provide some elements of an IoT service within the IoT service delivery chain.

Particular business risks include:

+ Contractual protections as to uses and disclosures of data may not be enforceable against third parties (that is, persons that are not parties to the contract with the data source), particularly given ready ability of service providers to move data to jurisdictions which have inadequate contract law systems and enforcement frameworks.
+ Release of data to facilitate research purposes may compromise entitlement of the data source to protection of this data as confidential (trade secret) information.
+ Loss of control of data may directly and adversely affect the business of the data source: for example, data may be used by competitors to more effectively target the data source's products, services or customers.
+ IoT service delivery chains and inter-working of IoT services with IoT communications services and devices, particularly services and devices supplied or managed by third parties, may create security vulnerabilities and weak points at which data may be compromised or intercepted.
+ Regulators or litigants may obtain access to the data for uses potentially adverse to the business.

There is also a significant prospect that concerns as to loss of control of data (for instance, that data may be used by competitors or others adversely to the interests of a data source or data controller), or as to information security of data as that data passes through the IoT service delivery chain, may significantly impede data sharing and provision of open IoT platforms and devices. Unless these concerns are adequately addressed, a likely outcome will be to advantage fully integrated IoT service providers, closing out opportunities for specialist or niche providers. This would likely be adverse to Australian start-ups and other Australian businesses competing with vertically integrated global operators that can operate 'closed system' IoT services and therefore do not need to address the diverse issues associated with data sharing within an IoT service delivery chain. In other words, effective and predictable legal protection (in Australia and in other markets) that facilitates data sharing within the IoT service delivery chain is likely to be more important to Australian start-ups and other Australian businesses than to vertically integrated global operators that provide 'closed system' IoT services.

The sharing of particular data fields or data sets between multiple entities (for example, a data analytics services provider, a communications service provider, a device provider, a data warehouse operator, and so on) also requires particular sensitivity as to consumer concerns. Consumers are concerned about collection and uses of personal information about them. However, their concerns do not begin and end with data privacy. IoT applications require trust between consumers and other affected individuals as to proper and sensitive handling of information about them by IoT service providers and all other entities involved in the IoT service delivery chain that have access to information about those individuals, including personal information. That trust is facilitated by good privacy management, including appropriate transparency and understanding of information handling practices.

Consumers will likely soon demand greater transparency than has been expected of businesses to date as to diverse uses of data, for example, as to the pricing of services as offered to different customer segments or classes of users, or as to disclosures to law enforcement agencies or private litigants. And while IoT services are becoming more complex and diverse, product lifecycles shortening and the number and range of participants in the IoT service delivery ecosystem increasing, businesses and consumers are demanding simpler forms of contract and more readily understandable operation and enforcement of consumer protection laws. IoT businesses also need predictable operation of intellectual property laws and competition regulation and availability of suitable radiocommunications spectrum for low powered devices in Australia and other markets that those businesses service.

Hence the many business and legal challenges of the Internet of Things.

**PETER G LEONARD**
**Partner, Gilbert + Tobin Lawyers, August 2016**


Sydney
Level 35, Tower 2
International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000

Melbourne
Level 22, 101 Collins Street
Melbourne VIC 3000

Perth
1202 Hay Street
West Perth WA 6005