Smart Grids: What are they and what are the emerging legal issues?

By John Gray and Vinod Sharma

John Gray *is a Partner at HWL Ebsworth. He is the national leader of the firm's Technology, Media and Communications group.*

Vinod Sharma *is an Associate at HWL Ebsworth.*

In an age when environmental concerns are dominating social, political and commercial agendas, the role that information technology might play in reducing carbon emissions is gaining widespread attention. The new vision of "green IT" has two aspects: first, a reduction of the global carbon footprint produced by IT infrastructure; second, the use of IT to help reduce the carbon emissions of other infrastructure and activities.

In the delivery of electricity to consumers, governments, energy utilities and energy industry observers are looking to "smart grids" – a term that describes varying degrees of electricity grid automation through information technology – to improve the efficiency, reliability and stability of energy transmission and distribution networks. It is hoped that smart grids will, in turn, help reduce carbon emissions through the reduction of energy consumption and wastage.

In Australia, on 30 October 2009, the Commonwealth government officially launched its plans to build Australia's own smart grid by inviting bids for its *Smart Grid, Smart City* project. This is a $100 million project where the federal government and the energy and communications sectors will collaborate to build Australia's first commercial-scale demonstration smart grid.

What is a smart grid?

A smart grid is essentially an intelligent electricity transmission and distribution network.

What makes it intelligent is a combination of information technology hardware, software and communications infrastructure which generates data about the operations of the network, and harnesses that data for more efficient operations.

The Commonwealth government in its pre-deployment report, '*Smart Grid, Smart City: A new direction for a new energy era*', considered that four principal categories of benefits could be identified from its proposed implementation of a smart grid in Australia:

1. direct financial savings;
2. reliability;
3. environment protection; and
4. customer empowerment.

In addition, it is estimated that an Australian smart grid would result in a minimum estimated gross benefit to the Australian economy of $5 billion annually.

A further benefit may be that smart grids will enable end users to generate and feed electricity back into the network.

What will be the opportunities for the IT industry?

The Vice President of Marketing for Cisco's Network Systems Solutions Group, Marie Hattar, provides an insight into the potential global scale of smart grids when she refers to a "...network [which] will be 100 or 1,000 times larger than the Internet. If you think about it, some homes have Internet access, but some don't. Everyone has electricity access - all of those homes could potentially be connected."

Smart grids around the world are still at a conceptual stage. The technology required to automate electricity networks is relatively undeveloped and governments, utility companies and the technology sector are currently working on demonstration implementations.

While smart grid technology remains at an evolutionary stage, a survey of current thinking indicates that there are three distinct network sectors to any smart grid:

1. consumer interfacing technology, including what has been coined the "Home Area Network";
2. 'smart' technology which facilitates the intelligence of the grid itself (for example, advanced metering infrastructure which feeds usage data through the grid back to substations; and self-correcting fault technology); and
3. information technology used by smart grid operators and utility companies to exploit the data generated through the smart grid – the "network intelligence" – for such purposes as adjusting electricity supply or

rates to certain end points during peak times; fault diagnosis; and customer billing.

The opportunities for the IT industry could arise out of the development of the hardware components of the smart grid and the software applications that will effectively provide the "intelligence" for the smart grid. This could involve anything from a visual display unit at an end user's house which shows energy consumption in real time by drawing data from appliances on the so called home area network; to software which identifies faults on the smart grid and automatically re-routes electricity through alternative paths on the grid; to applications which identify user consumption patterns and provide customer intelligence to utilities which in turn might offer special pricing plans or promotions to customers.

The legal implications

At this early stage, the emerging legal and regulatory issues associated with smart grids fall into five broad areas.

Information Collection and Handling

Smart grids will generate and collect both network intelligence and customer energy usage information. The latter class of information, including data about the amount of electricity a person consumes, their consumption patterns and, possibly, the types of devices they have connected to the grid, could be characterised as personal information under the privacy laws of Australia and many other countries.

Consequently, the collection of data from the smart grid, and its subsequent handling, will be regulated. The use and disclosure of such data may create significant regulatory risk for utilities and network operators.

Network Security

As with most modern computer based technologies, the network and other technology infrastructure comprising smart grids will be vulnerable to hacking, interception and other outside interference. This risk will be heightened by the geographical scale of smart grids, the likely diversity of smart grid technology and the sheer number of devices connecting to the grid from the home to the power station.

In addition to potential privacy breaches, the risks associated with failures in network security include fraud (for example, users tampering with network data to reduce their electricity bills), denial of power resulting in commercial damage to users, sabotage of the network and personal injury or property damage caused by interference with the proper functioning of devices connected to the network.

Consequently, legislators will need to regulate behaviour in relation to the smart grid. It is likely that this will be achieved through the application of criminal penalties to those obtaining unauthorised access to, or interfering with, the smart grid (e.g. similarly to criminal laws in relation to telecommunications interception or computer hacking). Commercial opportunities for the technology industry might be found in the area of smart grid security.

Control and Vulnerability

Many devices on smart grids will operate relatively autonomously, utilising artificially intelligent processes to generate actions with minimal human oversight and control. Some such devices might malfunction on occasions of interrupted power supply or unreliable network data – for example, a SCADA device that fails to monitor and control generation or transmission equipment, or a medical device connected to the grid from a patient's home – with potentially catastrophic consequences.

Those who manufacture, maintain or operate smart grid devices should consider the potentially significant legal risks that may be associated with sub-standard software engineering embedded in such devices, hardware malfunctions and external interference.

A software fault on a device connected to a smart grid might significantly amplify the already inherent danger posed by electricity grids. For example, a software design fault in one device may result in erroneous data being generated by that device. Such erroneous data may be used by a "smart" device to make electricity routing decisions in the smart grid. A "smart" electricity transmission device on the smart grid could potentially enter into a "loop", oversupplying electrical current to a particular segment of the grid, ultimately causing personal injury or property damage.

In such cases, it is possible that principles of the tort of negligence and product liability laws could hold the operator of the smart grid or the supplier of such technologies responsible for loss and damage resulting from device malfunction.

Standards

Standards will need to be implemented to govern the smart grid and the devices connected to it.

It is possible that devices developed for use on smart grids will become regulated and have to comply with standards set by law and supervised by a statutory body, as is the case for medical devices in Australia.

Supplementing such standards may be other industry based interoperability standards designed to ensure that devices on a smart grid are capable of interacting with other devices supplied by other manufacturers.

Early dominance in this space by one, or a handful of, smart grid device manufacturers using proprietary standards may create significant problems for the evolution of such technology and have the effect of diluting competition.

Take a hypothetical manufacturer of smart grid devices. In the current smart grids industry landscape, there are

no accepted interoperability standards or regulations mandating "open" standards. If that manufacturer were to gain market share using its own proprietary standards while the smart grid industry is in its infancy, this could create significant problems later for competitors and consumers as the technology matures.

Access and Jurisdiction

To maintain healthy competition in the electricity supply market, it is likely that those entities operating smart grid infrastructure will be subject to significant market regulation in a similar manner to the current electricity supply telecommunications industries.

For example, the Australian telecommunications industry is heavily regulated so as to promote competition. Regulations impose obligations on network operators to provide access to their networks to other telecommunications carriers and service providers and to provide interconnection of calls between networks.

In the case of smart grids, it is likely that a whole "national" grid will in reality be a proliferation of interlinked smart grids operated by multiple, competing operators. These will cross jurisdictional boundaries. It is inevitable that such an industry landscape will necessitate significant competition regulation, regulated on a national rather than State basis, and impose mandatory obligations on smart grid operators to share resources with, and provide access to, their competitors.

Final Thoughts

The advent of smart grids will bring significant commercial opportunities for energy utilities and benefits for consumers, and may help solve some of society's problems with carbon emissions. The IT and communications sectors, which are expected to provide the necessary intelligence and connectivity, also stand to gain. As energy utilities, governments and technologists grapple with the technical challenges of converting the smart grid vision into reality, lawyers will need to be alert to the emerging legal issues.

Federal Court loses its Sensis on Phone Directories

***Telstra Corporation Limited v Phone Directories Company Pty Limited* (2010) FCA 44**

By Peter Knight and Rebecca White

Peter Knight (Partner, Banki Haddock Fiora) *has over 25 years experience in information technology and intellectual property industries, in commercial advice and contract preparation and negotiation, as well as litigation and dispute resolution.*

Rebecca White (Senior Associate, Banki Haddock Fiora) *advises on a range of copyright and litigation matters including breach of contract claims, trade practices issues and copyright infringement.*

On 8 February 2010, her Honour Justice Gordon of the Federal Court of Australia found that copyright does not subsist in the White Pages and Yellow Pages directories ("the Directories") published by Telstra Corporation Limited and Sensis Pty Limited ("Telstra"), because Telstra had failed to establish to her Honour's satisfaction who were the authors of the Directories. Her Honour suggested that, if collections of data in any form were to be protected, then perhaps the apparent deficiency in copyright law could be filled by *sui generis* legislation.

Whilst the judgment reminds copyright lawyers of the importance of authorship and originality in any copyright claim, it is, with respect, deeply flawed on many levels.

Background

Emboldened perhaps by the decision of the High Court in *IceTV Pty Limited v Nine Network Australia Pty Limited*,[1] the issue of subsistence of copyright in the Directories had been separated as a preliminary question to be determined by the Court.

Central to Telstra's claim to copyright was the presumption as to both subsistence and ownership provided by s 128 of the *Copyright Act 1968* (Cth) ("the Act")[2] which provides: