Oil & Gas IP: The Perils of Theft, Joint Ventures and Patents vs. Trade Secrets

Whether it be pushing production optimisation through digital oilfield infrastructure or innovations in hydraulic fracturing, it is widely recognised that advances in oil and gas technology will be the major propellant for the industry’s success in the coming decades.

From bitumen and extra-heavy oil to shale and high pressure/high temperature wells, the fast pace of technological progress has meant that intellectual property in the conventional and unconventional arena, is worth its weight in black gold, and should be either zealously guarded or keenly acquired.

If you can’t beat ‘em, buy ‘em

With such a premium placed on intellectual property, the bigger players in the oil and gas business are spending big to both foster and capture emergent intellectual content from companies at the forefront of industry innovation.

In September 2013, California-based supermajor Chevron announced the launch of Chevron Technology Ventures Fund V, a $90 million endowment “to invest in early- to mid-stage companies and in limited partnership funds.” According to CTV President, Barbara Burger: “We are using venture capital as a conduit for early adoption of emerging technologies and to build a pipeline of innovation for Chevron.” Fund V is an adjunct of Chevron Technology Ventures LLC, founded in 1999 to invest in start-up companies whose
innovations could significantly benefit Chevron’s existing businesses and lead to new growth opportunities.

In the same fashion, Prometheus Energy, one of the fastest growing suppliers of liquefied natural gas (LNG) to the industrial sector in North America, is privately held and equity financed by Shell Technology Ventures Fund 1 B.V. and Black River Asset Management LLC, a wholly owned but independently-managed subsidiary of Cargill. Prometheus have recently pioneered the construction and deployment of the first 100 per cent LNG-powered turbines for hydraulic fracturing in South Texas’s Eagle Ford Shale Play.

Once you have developed or acquired your intellectual property, the next step is to protect it.

**Trade secrets vs. patent protection**

Oil and gas innovators will come to a fork in the road when deciding how to best safeguard their intellectual property: one prong will take you towards patent protection, the other down the path towards protection as a trade secret. Both routes are mutually exclusive and the best track to beat will depend on the type and stature of the company you work for, be it operator, service provider or tech firm.

As with any secret, protection of information is only viable if the interested parties keep schtum and maintain that confidentiality. As soon as secret information is disclosed and enters the public domain either intentionally or unwittingly, commercial exploitation is fair game as any protections are vitiated.

Given the nature of the business, the trade secret route may be a better option for operating companies as they are less likely to be in a position to develop and share technology with third parties. However, by their very makeup, service providers and tech
companies will have multiple touch points with organisations across the sector and are, therefore, more susceptible to loss of trade secret protection.

In the contemporary industry, operators, contractors and ancillary third-party organisations form transient alliances across an increasingly global marketplace. A “revolving door” exists in the sector, with employees regularly moving from one company to the next and across verticals. When employees leave, often trade secrets depart with them and confidentiality is compromised, proving to be a stumbling block for the trade secret approach.

Problems may also arise in the course of “the race to innovate”, with many competing parties independently vying to develop the same technology. If any of these parties divulges the details of their findings, other runners in the race may have their own efforts in the area exposed, rendering trade secret protection unworkable.

For all of the reasons above, patent protection, with exclusive rights granted to an inventor for a limited period of time in exchange for the public disclosure of said innovation, is the preferred modus operandi for most oil and gas intellectual property protection.

**Joint Ventures**

A joint venture (JV) can be defined as “an association of corporations or other legal entities who agree by contract to engage in a common undertaking for joint profit over a specified length of time.”

Typically less economically and politically risky than full organisational mergers, JVs are an entrenched feature of the oil and gas industry, and are becoming increasingly prevalent between Western and Far Eastern companies and NOCs. A good example of this can be seen in the US shale plays, where foreign companies have invested $26 billion in the past five years in 21 JVs with domestic partners.
The nature of fixed-term collaborations that do not have a permanent legal status throw up unique problems in the realm of intellectual property, below we look at three of these:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who owns the IP?</strong></td>
<td>When it is unclear which parties have contributed to, improved or developed intellectual property, disputes may arise that can hinder or sunder otherwise profitable projects.</td>
<td>Regular and detailed progress reports should be made during the lifespan of the venture. A single individual or group should be tasked to martial these updates and manage the intellectual property in accordance with the stipulations of the joint venture agreement.</td>
</tr>
<tr>
<td><strong>Who works for whom?</strong></td>
<td>Are employees acting on behalf of the joint venture or one of the venture partners? Or, have individuals extraneous to the venture been contracted to the joint venture? Typically, intellectual property created in the course of employment is owned by the employer. However, if it is not clear who the employee is acting for when the intellectual property is created, then who the rightful owner is may become a grey area. Usually, unless expressly assigned, contractors will own their intellectual property, and without suitable agreements, the ownership of intellectual property elaborated during a project may reside with multiple parties.</td>
<td>This can be accomplished by a clear separation of powers. Crystal clear job descriptions and a segregation of responsibilities is crucial, even siloing employees in separate offices with separate computers and logins to make sure there is no cross pollination between the work they do for a single partner and then the joint venture itself.</td>
</tr>
<tr>
<td><strong>Cui bono? Who benefits?</strong></td>
<td>A common pitfall is the failure of joint venture parties to account for such profits and create a mechanism for collecting and distributing them after the joint venture is concluded. Intellectual property created in the joint venture may continue to generate revenue after the project is concluded, for example by way of licenses to third parties.</td>
<td>A separate legal entity should be incorporated to manage any on-going royalty arrangements or profits from any intellectual property created in the course of the joint venture. This will also act as a way to manage liability and as a conduit for the payment and handling of the costs of legal protection from trademarks and patents, to industrial design or copyright registrations.</td>
</tr>
</tbody>
</table>
Intellectual property theft exists in two strains: internal and external. Internal theft is usually
the province of the notorious Disgruntled Employee or an “enterprising spirit”. In the
Information Age, external theft exists as incursions and breaches of network security.

So grave has the problem of cyber crime become, that in a recent Oil & Gas IQ survey
completed by global CIOs, cyber crime was deemed to be the biggest menace to companies
in the sector, almost twice as much of a concern as cyber espionage and cyber warfare
combined.

This is in no small part due to the Night Dragon cyber attacks, a string of major cyber
assaults starting in November 2009 that targeted oil, energy and petrochemical companies.
According to McAfee, the attacks were “coordinated, covert, and targeted” with intruders
collecting gigabytes of proprietary and highly sensitive information over a period of months.

Today it is estimated that more than 80 per cent of a company’s information is stored
electronically and 75 per cent is never printed. Most work environments are open sourced
to facilitate collaboration between team members. However, a cooperative milieu that
promotes ease of access to electronically-stored information (ESI) also provides multiple
access points for larceny via USB thumb drives, external hard drives or email.

In the USA, a recent study by the U.S. Federal Bureau of Investigation found that instances
of intellectual property theft by employees had increased considerably since the first pangs
of the economic downturn in 2008. A staggering 44 per cent of companies surveyed had
experienced internal theft of intellectual property in 2012.

In illustrative example of this can be found in the case of Glenn J. Soileau, a former
employee of two subsidiaries of General Electric Oil and Gas. Soileau smuggled out more
than 3,700 files containing pictures, diagrams, and other information relating to tools and
equipment used in oilfield exploration work and brought them to his current company,
Advanced Electronic Services. On confessing to the theft, Soileau faces a maximum of five years in prison, a $250,000 fine, restitution, and three years of supervised release for the count of unauthorised access to a protected computer.

Three ways to make internal IP theft harder

Mr Soileau was not the first, and will not be the last member of staff to breach the confidence of his employer and make away with private information. Employee theft of intellectual property may often fly under the radar, so how can you keep tabs on the actions of your employees without Orwellian levels of surveillance? Here are three easy ways to make it harder for your employees to profit from business critical proprietary information.

1) Highlight your IP policies at all points of your employment cycle

Make sure that new hires are fully aware of your internal intellectual property and confidentiality policies from the outset, and don’t let them forget it. These policies should be core to employment contracts and expressed clearly. Periodic reiteration of these policies is crucial to create a climate of transparency in which employees are fully cognisant of the rules, and the penalties for infraction of those rules.

Likewise, when an employee leaves the company either willingly or unwillingly, there should be increased examination of his/her actions prior to exit.

2) Identify high-risk individuals for scrutiny

To some degree, most employees in an organisation will have access to information that would be beneficial in the hands of their competitors. However, there will be some employees that are in more of a position than most to get their hands on sensitive information – such as those in higher management with guiding roles in strategy, sales representatives whose contact lists contain essential customer data and those on the front lines of research and development that are fomenting new proprietary technologies.

These high-risk positions should be the target for specific surveillance and forensic computer investigation to make sure that confidential data does not leave the building if and when they do.

3) Data by itself is not evidence – act quickly

When it comes to collecting proof to prosecute for intellectual property theft, evidentiary standards necessitate detailed chronological documentation of everything that happened to the data in question. Any file modification or completed commands such as viewing, printing and saving files will permanently change the metadata that acts as a record of activity.

There are simple ways to remove temporarily stored data and altering metadata is also not beyond the reach of those with a good grasp of IT, making erasure of ones tracks eminently
feasible. To combat this, computer forensic processes should be in place in order to identify, preserve, recover, analyse and present facts and opinions about the information in accordance with the usual requirements for digital evidence: authenticity, reliable obtainment, and admissibility.

Time is of the essence in order for any legal action to be effective - the longer the gap between commission of the theft the more chance there is for any evidence of wrongdoing to be expunged.

****

For more information on this topic, attend the Oil and Gas Intellectual Property Summit - the only dedicated event dealing specifically with intellectual property challenges within the hydrocarbons industry - this 27th-29th January 2014 in London, UK