

REPRINT

CD corporate
disputes

TRADE SECRET LITIGATION

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
JUL-SEP 2016 ISSUE



www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

Bird & Bird

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com
© 2016 Financier Worldwide Ltd. All rights reserved.

MINI-ROUNDTABLE

TRADE SECRET LITIGATION



PANEL EXPERTS



James Froud
Partner
Bird & Bird LLP
T: +44 (0)20 7415 6000
E: james.froud@twobirds.com

James Froud is a partner in Bird & Bird LLP's International HR Services Group, based in London. His practice is unusually diverse; he advises on all aspects of contentious and non-contentious employment law at all stages in the employment cycle, supporting a broad range of clients including multinational corporations, public sector bodies and also individuals.



Christopher Gerardi
Senior Managing Director
FTI Consulting
T: +1 (212) 499 3638
E: chris.gerardi@fticonsulting.com

Christopher Gerardi is a senior managing director at FTI Consulting and is based in New York. Mr Gerardi is the co-leader of the FTI Consulting Dispute Advisory Services and Intellectual Property practices. He has more than 25 years of experience assisting companies and plaintiffs' and defendants' counsel with complex economic, financial, accounting and litigation issues.



James Pooley
Founder
James Pooley PLC
T: +1 (650) 285 8520
E: james@pooley.com

James Pooley is a litigator with almost 40 years experience in trade secret and patent matters. A former Deputy Director General at WIPO, he has authored several books on trade secrets, most recently *Secrets: Managing Information Assets in the Age of Cyberespionage* (Verus Press 2015). He was deeply involved in the legislative process leading to the Defend Trade Secrets Act, including testifying as an expert witness to the US Senate Judiciary Committee.



Brian Hinman
Chief IP Officer
Royal Philips
T: +31 6 15 870498
E: brian.hinman@philips.com

Brian Hinman is chief intellectual property officer of Philips, where he leads a worldwide team in conducting intellectual property management, strategy, litigation, standards, patent portfolio management and IP monetisation. Mr Hinman previously co-founded Unified Patents Inc, served as vice president of IP and Licensing at InterDigital and also vice president of IP and licensing at Verizon. Mr Hinman was also the founding CEO of Allied Security Trust (AST), vice president of IP and licensing at IBM and director of licensing at Westinghouse.



David Koris
General Counsel
Shell International Limited

David Koris has been an intellectual property counsel for over 30 years with broad experience in all phases of IP practice. For the last 10 years he has served as the executive vice president and general counsel of IP for Shell International B.V. Located in The Hague, Mr Koris is responsible for the global protection of the Shell brand as well as IP asset management including IP asset development, enforcement and licensing. In addition to managing the IP organisation, Mr Koris is a partner in the technology planning team.

CD: Reflecting on the last 12-18 months, could you provide an overview of trade secret litigation activity? What overarching trends and developments have you witnessed?

Froud: The number of cases involving employee competition, breaches of confidence and team moves has remained steady during this period. From this activity it is possible to discern a trend of judicial sympathy towards employers. The courts have regularly shown willingness – wherever possible – to protect businesses and to uphold reasonable restrictions contained within contracts of employment. Interestingly, the litigation has not been focused in one or two specific sectors. We have also seen indications that arbitration is becoming a more popular way of resolving commercial trade secrets disputes, especially where international parties and transactions are involved. This is driven in part by the fact that arbitration proceedings are generally – but not always – confidential and the relative ease of enforcing any award.

Gerardi: We have seen a steady increase in trade secret litigation and even more arbitrations given the recent changes to US patent laws, and given that the Defend Trade Secrets Act (DTSA) was recently signed into law, there will surely be even more activity going forward. The Supreme Court has ruled on several

patent-related matters, such as *Alice Corp vs. CLS Bank*, *Octane Fitness vs. Icon Health & Fitness* and *Limelight vs. Akamai*, increasing the volume of patent litigation. Further, the America Invents Act, which was signed into law September 2011, provides for tougher patent review proceedings. These changes to patent law have made it more difficult to enforce patents. The value of intellectual property, however, continues to increase. We see more clients actively debating whether to try to protect their IP through patents, or whether they might better keep the information secret and protect it under trade secrets law. I believe the passage of the DTSA will reinforce the inclination to keep some IP as a trade secret. Clients' desire for secrecy is also why we are seeing an increase in the number of private arbitrations, which can be kept out of the public eye, compared to litigation, which is in a public forum.

Koris: We do not have a lot of trade secret litigation happening at Shell which I attribute to the training and processes the company has in place around developing technology with partners and the disciplined approach that is taken toward information management. Where there have been contested issues, they usually spring from misunderstandings that develop around the information that is disclosed pursuant to a non-disclosure agreement but which is found to be of either of little interest to us from a technical perspective, already known to us from prior

developed efforts or those circumstances where it is determined that the information is already in the public domain. I see the issue of information management and security to be a top priority for most IP leaders whether they support large multinational corporations like Shell or support a new start-up.

Hinman: Although we have no recent statistical information from which to draw, our impression is one of an increase in trade secret enforcement on both federal and state levels within the US. Such enforcement almost always involves a party known to the owner of the trade secret concerned, for example, an employee, an ex-employee, or a business partner. Trade secret enforcement actions against employees appear to be more prevalent on a state rather than federal court level. We have also observed that state court cases more often are directed to misappropriation of internal business trade secrets, such as customer lists, whereas federal court cases typically deal with theft of technical trade secrets, such as technical information and know-how, the latter often being coupled with other federal causes of action such as claims for patent or copyright infringement. In Japan, protection of IP by maintaining it as a trade secret rather than by filing for a patent is being considered more often, especially in view of two recent trade

secret cases, *Toshiba vs. SK Hynix* and *NSSM vs. Posco*. In Europe, due to the lack of a harmonised legal framework, the picture is less clear.

“Trade secret enforcement actions against employees appear to be more prevalent on a state rather than federal court level.”

*Brian Hinman,
Royal Philips*

Pooley: Two important trends have surfaced recently in trade secret litigation. The first, exemplified by the *Epic vs. Tata* verdict in Wisconsin in April, is larger damage awards. That case produced a verdict of \$940m and is one of several outcomes in the nine figure range in the past few years. Using information gleaned from electronic discovery, counsels seem to be taking advantage of the relatively flexible and generous rules on damages in trade secret cases. The second trend, perhaps influenced by the first, is third-party financing of trade secret litigation, allowing plaintiffs to hire more capable counsel and continue to fight through trial. An example is the Minnesota

verdict against Caterpillar last December, in which a jury awarded \$75m to a small UK company that claimed its business had been ruined by Caterpillar's misuse of secret product information. The case was prosecuted by a top tier law firm hired by a litigation finance group.

CD: In your opinion, do companies place enough importance on protecting their trade secrets? Are malicious actors continually evolving the methods they use to steal them?

Gerardi: Most companies recognise the importance of trade secrets, and I believe many struggle to keep pace with how to best protect them in an age of portable electronic devices and cloud storage. For example, some companies allow employees to connect personal mobile devices to corporate networks, through which they can access, upload and download data files. That approach may provide certain mutual benefits, such as convenience, greater flexibility and productivity. However, companies need to be aware of the increased risks this practice imposes, including data security issues and heightened opportunities to carry out mischievous acts. In addition to employee-initiated actions, we are seeing an increase in more sophisticated hacking of company networks to obtain all types of proprietary data by organised crime, foreign companies and foreign governments.

Such malicious actors are well funded and very sophisticated.

Koris: We have a high level of focus on information management and trade secret management, which is becoming more of a concern to senior business leaders. This initially may occur due to concerns over the risk of having their IT systems hacked. Best practices for defending against cyber intrusions are continually advancing to meet the challenge. As senior leaders become more familiar with the requirement for continually improving the steps they take to secure their data, inevitably the focus shifts to the broader topic of information management. What level of security is sufficient? The answer to this depends on the business and industry. For a large corporation with a number of businesses, a single approach may be too light a touch for some and too restrictive for others. Eventually, the issue of information security turns to the scope and location of the types of information that need to be protected. When a conversation turns to trade secrets, often highly valuable secret processes and formulas come to mind. While technical trade secrets associated with oil and gas reserves require a high level of security, a high level of security is also needed for the management of strategic business planning information, pricing information and the personal data of employees.

Hinman: Generally, in the digital world, the value and importance of trade secrets has increased. In accordance with that development, there is an increased need for optimal protection for technical innovations, such as computer algorithms and source code, in addition to sensitive business information. The importance of protecting trade secrets cannot be stressed enough. At the same time, the digital world poses challenges for protecting trade secrets. For example, more and more information is stored in cloud based systems that are vulnerable to unauthorised remote access by way of increasingly sophisticated techniques. Therefore, relying on general IT security measures is no longer sufficient for protecting electronic information and preventing theft of valuable trade secrets. For effectively combating malicious actors, businesses and public authorities should establish secure IT environments in which the methods for protection are continuously evaluated and upgraded.

Pooley: I believe that too many businesses fail to address their trade secret risk exposure until after they have been hit by a substantial loss. Intangible assets now represent over 80 percent of the value of public companies, up from 20 percent in the 1970s. And all this critical information is stored on globalised networks linked to hundreds or thousands of access points – laptops, tablets and smart phones. As with money held by banks, data cyber thieves go to where the most valuable assets are stored,

and they are constantly adapting their techniques for penetrating company computer systems, testing defences with automated attacks. Once inside, hackers secretly install malware that can sit unnoticed for months while it surveys, collects passwords and sends out collected data.

Froud: Companies value their trade secrets enormously. However, precious few companies take adequate preventative steps and too many rely, erroneously, on a reactive approach which is often employed too late. The prospects of a business successfully protecting its confidential information from misuse by nefarious employees will normally rest on the extent to which an employer has undertaken the unglamorous but prudent safeguarding tasks. It remains to be seen whether the Trade Secrets Directive – which needs to be implemented in EU member states within the next two years – will herald a change in approach. The methods used to misappropriate trade secrets have undoubtedly evolved. This is due in part to the nature and form of information and data changing with the digital age. It is now much easier for employees and third-parties to collect, intercept and transfer information. Cyber security is increasingly becoming a concern and the sheer volume of data can offer opportunities to hide unlawful activity. However, the advance in data forensics technology – together with the legal tools available, if properly

deployed – probably gives companies an edge against malicious actors.

CD: In your experience, what are the most important aspects that need to be observed when developing a strategy for protecting trade secrets and managing related risks? What tools are companies utilising?

Hinman: It is important to recognise that measures protecting trade secrets may be obtrusive and have an impact on the conduct of business. Therefore, it is key to find the right balance between restricting access and allowing normal business operations to continue. In doing so, a one-size-fits-all approach will probably not work. The choice of the appropriate measures in a particular situation also may hinge on the perceived value and sensitivity of the trade secret concerned. That is, while for certain information, standard protective measures such as confidentiality agreements, appropriately drafted exit undertakings for key positions and providing access on a need to know basis only, may suffice, for the most sensitive type of information, more sophisticated, restrictive, protective measures will be needed. Also, companies would be well advised to conduct regular internal audits on the compliance with any protective measures, as well as to educate

employees on the importance of protecting trade secrets and on the protocols developed for this purpose.

“The most cost-effective preventive techniques involve employee training, policies for on-boarding of new hires, and close management of outside relationships where confidential information is shared.”

*James Pooley,
James Pooley PLC*

Pooley: Proper risk management looks at the dual threats of unwanted contamination by new employees hired from competitors and of data loss from carelessness or even hacking. Protecting a company’s computer systems requires the installation of software tools not only for prevention but also detection and rapid response to breaches as they occur. Employee-owned mobile devices like smart phones should be subject to monitoring software that allows remote wiping of data. But beyond the technology, businesses also need to apply old fashioned people management skills, because the vast majority of information loss occurs not through espionage but simple carelessness. As a result, the most cost-effective preventive techniques

involve employee training, policies for on-boarding of new hires, and close management of outside relationships where confidential information is shared.

Froud: The very first step in any protection strategy is to identify the relevant trade secrets. It is only once an inventory has been prepared and the assets have been mapped that an organisation can take truly meaningful steps to protect the information and to mitigate risks. When this stage is completed it will be possible to undertake a risk assessment and to put in place the building blocks for robust defences and response mechanisms. From an employment perspective this is likely to involve an overhaul of employment contracts, a review of company policies focused on specific activities and behaviours, consideration of reporting lines and authorisation levels, varying access permissions and implementing cultural changes. Organisations may also look at technological solutions for tracking their data and engage with IT experts accordingly. We are seeing clients invite us and other relevant consultancies to undertake trade secret audits in order to assist with mapping, policy implementation and the creation of incident response teams.

Koris: In developing a strategy for protecting IP assets, the strategy must be aligned with the relevant business plan objectives. This presumes

that there are sound management practices in place to develop the technology and related intellectual property. So determining that there is a strong alignment in the business planning cycle between the projected economics, the anticipated benefit of new technical solutions, the commercialisation or deployment plans and the associated IP strategies is fundamental to success. The IP strategies also need to establish the scope and nature of the IP assets and provide a means of assessing whether the IP assets are being developed in the right areas of the technical value chain. The form of IP assets selected plays a role in supporting commercialisation or deployment plans. In some cases it may be prudent to have a higher number of patents in critical areas of the value chain as opposed to trade secrets.

Gerardi: Remarkably, the most basic aspects often get overlooked – physically isolate and protect your company's trade secrets and restrict access to employees with a business-related need to know. Mark documents and electronic files containing confidential and trade secret information with the appropriate legal and business notices. Before providing confidential information to outsiders, such as potential business partners, carefully consider how that information will be revealed and when and how it will be returned. Make sure you know the intended recipient and use confidentiality agreements. Outsiders should be given access to the least amount of confidential

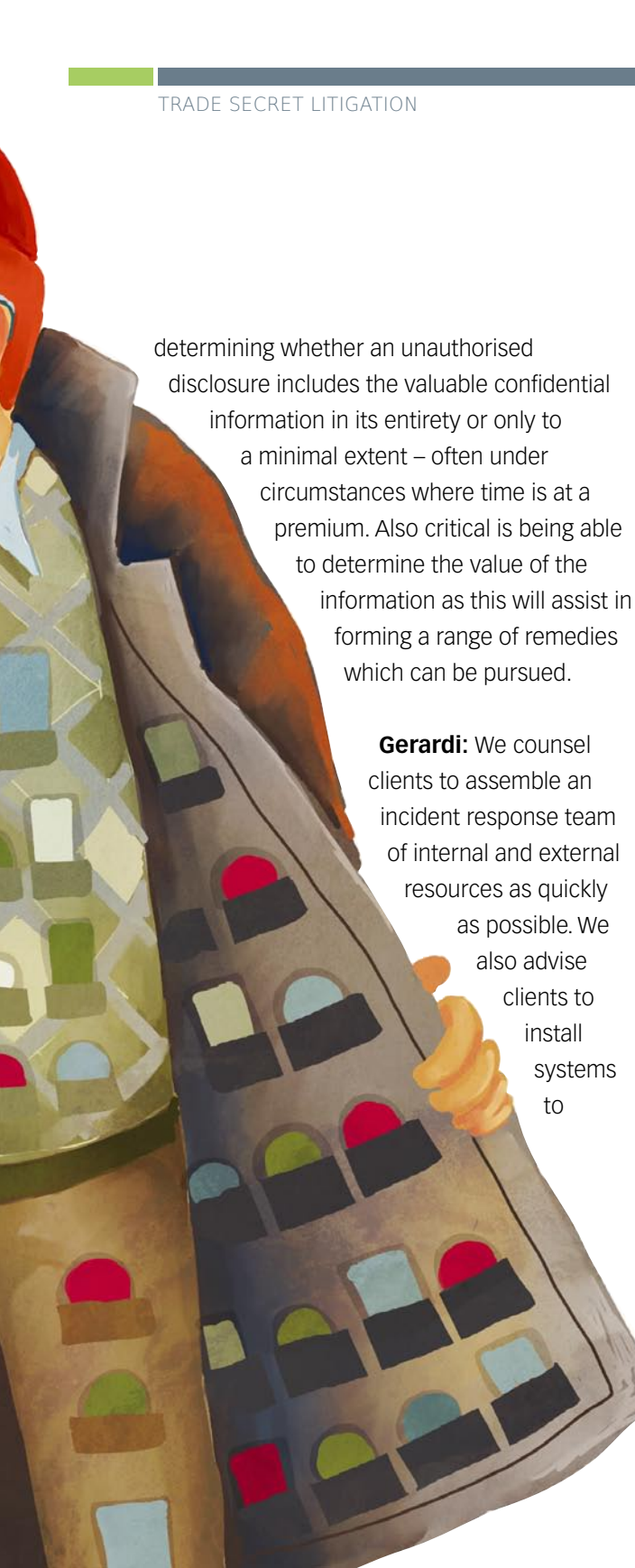
information necessary to achieve your objectives. Finally, formulate procedures to handle unsolicited disclosures. Litigation is often triggered by the receipt of unsolicited information and ideas from third-parties. To avoid claims that unsolicited information was stolen or that a confidentiality obligation was breached, a company should establish and communicate procedures to manage unsolicited disclosures. The procedures may include notifying persons submitting unsolicited information that your company will not enter into a confidential relationship; requesting that the submitter sign an acknowledgement that your company owes no duty of confidentiality; and alerting your company's legal department or counsel if an unsolicited submission relates to ideas or inventions that the company is presently developing.

CD: What initial steps should a company take if trade secret misappropriation by a former employee or third party is suspected or identified? Should they assemble an incident response team, for example? And what temporary remedies might be available?

Koris: If a situation would occur where some valuable information from an organisation has migrated out of the organisation to a competitor from a former employee or consultant, the first inquiry in this process is to assess whether the

human resources organisation has a record keeping system which enables the rapid retrieval of on-boarding and off-boarding documents. This is critical if it is desirable to secure injunctive relief from a court. Equally important is knowing what technology has been misappropriated. Having an information database which defines the metes and bounds of highly valuable confidential information such as a technical trade secret can provide a means of



A stylized illustration of a person wearing a patterned jacket, holding a large, colorful, abstract object that resembles a piece of fabric or a large, multi-colored letter 'A'. The object has various colored sections (red, green, blue, yellow) and is held by a hand with yellow gloves. The background is white with a green and blue horizontal bar at the top.

determining whether an unauthorised disclosure includes the valuable confidential information in its entirety or only to a minimal extent – often under circumstances where time is at a premium. Also critical is being able to determine the value of the information as this will assist in forming a range of remedies which can be pursued.

Gerardi: We counsel clients to assemble an incident response team of internal and external resources as quickly as possible. We also advise clients to install systems to

monitor where trade secrets may be housed and enable logging features that may be useful later on. Many clients have proactively identified these teams in advance of an incident, so that if and when an incident arises, they know whom to contact. The team includes internal IT, outside counsel, computer forensic resources and internal stakeholders. As appropriate, supplement the team with additional experts. Start by trying to triage things that need to be done – for example, any evidence that could be overwritten, removed or destroyed in the normal course of business should be preserved as quickly as possible. Depending on the circumstances and findings, you can seek a TRO to prevent the employee from using the data at a different employer.

Froud: In the event that employees are suspected of malfeasance, the employer needs to act on initial priorities. First, gather and preserve evidence, as quickly and quietly as possible, and, if there is an immediate threat to the business, and a sufficient level of knowledge to proceed, to isolate the individuals by identifying potential informants who are willing to cooperate against the malicious protagonists. Evidence is the key to any successful action and it is therefore imperative that appropriate steps are taken to secure it. We do recommend that companies establish a 'standing' incident response team – however, this is rare in our experience. The approach of most businesses is very *ad hoc*.

Temporary remedies will include immediately suspending individuals to enable investigations to be undertaken; seeking undertakings in relation to their activities and, if necessary, applying to the court for an interim restraining injunction.

Pooley: When trade secret misappropriation is suspected, the company often has to balance its need to understand what has happened with a need for rapid response. As a first step, experienced legal counsel should be called in to make an immediate assessment and begin an investigation. If the theft is not yet complete – for example, the company has learned that an employee is about to leave with confidential data and travel abroad – there may be grounds to ask a federal court to order law enforcement to seize the material, under the recently-enacted Defend Trade Secrets Act. In less extreme cases it may be sufficient to confront the employee or business involved either to prevent or mitigate the harm. In any event, the most effective response will be based on solid investigation and objective assessment by an internal team drawn from legal, HR, security, R&D and executive ranks.

Hinman: When a potential misappropriation is suspected or identified, making a comprehensive assessment should be given high priority, also because computer forensic evidence can be lost due to recycling of computer hardware and the overwriting of server data. A well-trained response

team should immediately initiate actions such as early capturing of electronic information from the misappropriator's electronic systems, including laptop hard drive, or analysing the nature and scope of a breach of IT security systems. For employees who move or have moved to a new employer, a prompt letter also may be recommended. Most reputable companies can be expected to take prompt action to quarantine a newly-hired employee when faced with credible claims of misappropriation from his or her former employer. Trade secret claims are well suited to temporary injunctive relief which should be among the immediate remedies sought. The fact that the dissemination of trade secret information may result in irreparable harm presents a compelling argument for temporary injunctive relief in relation to the misappropriation of trade secrets.

CD: What role does technology tend to play in trade secret litigation, such as using computer forensics to investigate suspected theft? What are the associated challenges and issues that companies need to consider in this regard – particularly in terms of preserving forensic evidence for admissibility in court?

Gerardi: Forensic evidence should be appropriately preserved as soon as possible. It is

better to have an expert do this properly than to risk modifying the data by looking at it yourself. Your forensic expert will also be able to validate his or her work and use court-accepted tools should testimony or regulatory review be needed. Typically, a forensic expert can identify many, but not all, actions taken on a computer. For this reason, consider meeting with IT or a forensic expert in advance of an incident to enable logging features that would be useful later on. For example, by default, a Windows computer does not log the name of files printed, but this can quickly be implemented across an organisation with little effort. Another example is that Windows doesn't log files copied to an external hard drive, but may track file access on an external hard drive.

Froud: Technology is playing an increasingly important role in trade secret litigation. The use of digital forensic experts is now commonplace in 'team move' and employee competition cases. The ease by which large volumes of electronic data can be moved, shared and deleted means that unscrupulous conduct would be more likely to go undetected without computer forensics. Unfortunately, the need to deploy such expertise leads to an inevitable increase in costs. Also, lawyers and computer scientists often communicate in slightly different languages which can create

challenges for the legal teams. It is therefore important to instruct legal counsel familiar with working with forensic teams. The ability to 'capture'

"The use of digital forensic experts is now commonplace in 'team move' and employee competition cases."

*James Froud,
Bird & Bird LLP*

digital images of hard drives and other electronic information without affecting underlying metadata is also important to ensure that the integrity of evidence can withstand scrutiny. In addition, data captured from fragments on a hard drive, including communications via personal emails accounts, is generally lawful and will not be subject to admissibility challenges.

Hinman: Computer forensic evidence is often indispensable and usually presented in cases involving the misappropriation of trade secrets. Forensic capturing of information should be handled by an independent professional forensic investigation firm rather than by the company's

internal IT department. While many IT departments may be capable of the technical demands associated with the capture and preservation of electronic information, forensic investigation firms are more familiar with the issues associated with the successful preservation of electronic information with a view to the admissibility of evidence in court. In addition, external firms are in a better position to review the actions of the company's employees independently and to assess the adequacy of the company's IT security systems and protocols.

Pooley: In response to misappropriation, and especially where litigation is anticipated, counsel will usually issue a 'litigation hold' letter to the company, to ensure that relevant records are maintained. Often this will be coupled with immediate copying of relevant hard drives and other electronic devices, so that forensic tools can be applied to learn how specific information may have been improperly accessed or compromised. Making these copies therefore serves the dual purpose of preserving evidence and informing the necessary investigation. Of course, it means that some system resources and devices will become unavailable for short periods of time, so some coordination may be necessary to ensure that critical services are not interrupted. For the most reliable results, evidence preservation should

be handled by an outside vendor working under the direction of legal counsel.

"Computer forensics plays a significant role in determining the businesses that are offering counterfeit products. This issue is a real challenge for prosecutors and IP practitioners alike."

*David Koris,
Shell International Limited*

Koris: Information removed from a company without authorisation can be difficult to identify. Certainly IT forensics is needed, particularly where efforts have been made to encrypt the information. This is also becoming a significant issue for anti-counterfeit work particularly where large volumes of good including counterfeit goods are being purchased through an internet provider. Computer forensics plays a significant role in determining the businesses that are offering counterfeit products. This issue is a real challenge for prosecutors and IP practitioners alike.

CD: Have there been any recent legal and regulatory developments affecting

trade secrets and related litigation? In what ways are companies using the law to pursue those suspected of stealing trade secrets?

Pooley: In the US, the most important recent development in trade secret litigation occurred on 11 May 2016, when the president signed the Defend Trade Secrets Act into law. Trade secret cases can now be filed directly in federal court, without having to rely on diversity or supplemental jurisdiction. Particularly in cases that involve actors in other states or countries, trade secret plaintiffs can now take advantage of the nationwide service of process and identical rules of procedure that apply in federal courts, along with the greater experience of those courts in deciding sophisticated questions of personal jurisdiction. And, in extraordinary cases of threatened misappropriation, plaintiffs may be able to secure an *ex parte* order to seize secret material before it is taken. Importantly, the DTSA also provides immunity to employees who reveal company secrets when reporting possible crimes to law enforcement, and requires businesses to give notice of this immunity in all employee confidentiality agreements.

Gerardi: By wide margins, the US House of Representatives and Senate each recently voted to pass the Defend Trade Secrets Act (DTSA) which, for the first time, would allow parties to file civil

lawsuits for trade secrets theft in US federal court. Unlike patents, trademarks and copyrights, trade secrets actions are currently under the jurisdiction of the states, and though most follow the Uniform Trade Secrets Act, there are still major state-to-state differences in application of the law. The DTSA will not pre-empt state laws already on the books, but will coexist with them. Its primary goal is to harmonise the law through a single federal statute, allowing for the development of more predictable, nationwide case law, and provide more certainty for those who are party to a trade secrets lawsuit. As noted, it also gives litigants easier access to federal courts, which some say are better equipped than state courts to handle cross-state and international cases, as well as complex technological issues.

Koris: If you look across the globe, many nations are moving ahead with national IP strategies which include the development of laws and regulations governing trade secrets. What comes to mind in particular is the European Union Directive for Trade Secrets and the Defend Trade Secrets Act of 2016 in the US. While the question deals with the enforcement side of the equation, the ultimate goal of information management and security practice is to enable the best forms of IP assets to be created to enable a business to leveraging the optimal value from the information generated. Again, the information can be of a technical nature and perhaps be considered a trade secret, or it can be the private

information of the employees of a company. Both forms of information need to be managed to ensure that full value is realised by the company and under those circumstances where regulations have been put in place requiring certain information practices, avoid hefty fines for non-compliance.

Hinman: In the US, the most important recent development is the adoption by Congress of the DTSA, a bill which President Obama recently signed. This piece of legislation creates a single US standard for protecting companies from trade secret theft through civil recourse including injunctions, compensatory damages as well as exemplary damages and attorney's fees in the event of wilful and malicious misappropriation. In Europe, the European Parliament has recently approved a draft EU Trade Secrets Directive that will likewise harmonise the legal measures available in case of trade secret misappropriation throughout the EU. In Japan, a revised Unfair Competition Law has become effective as of 1 January, enhancing protection of trade secrets while in China, draft amendments proposed to the Law against Unfair Competition will affirm current court practice regarding trade secret misappropriation. Further, discussions regarding a unified Chinese trade secrets law are ongoing. These legislative developments reflect recognition, on a global basis, of the need for effective civil recourse in combating the ever growing threat posed by trade secret misappropriation.

Froud: In the EU, a directive to harmonise and upgrade European trade secret laws was formally adopted by the European Council in May 2016 after the EU Parliament voted to adopt the proposed wording on 14 April 2016. This Trade Secrets Directive has been introduced because the European Commission, supported by industry, were concerned about the inconsistent levels of protection across the EU and the effect this was having on innovation. Only around two-thirds of EU states have specific legislation concerning the misappropriation of trade secrets and in some countries there is more than one definition of a trade secret, depending on the legal context. The Trade Secrets Directive will harmonise laws across the EU, adopting the 1994 WTO TRIPS definition of a trade secret, which is also reflected in the definition adopted by the US in the Uniform Trade Secrets Act and most recently in the DTSA. This definition is more prescriptive than currently used under English common law and includes requirements that, in addition to being 'secret', the information has commercial value because it is secret, and has been subject to reasonable steps in the circumstances, by the person lawfully in control of the information, to keep it secret. This last point is one which companies will need to address from a practical perspective to ensure that their trade secrets are protected. Meanwhile, the UK government has opened a consultation seeking views on whether non-compete clauses in employment contracts stifle innovation.

CD: What final piece of advice can you offer to companies in terms of protecting and enforcing their trade secrets through litigation?

Hinman: Companies should identify and catalogue the trade secrets that they own. Whenever possible, key business leaders should be involved in this exercise. It is also important that companies establish and implement appropriate protocols for employees setting out the rules and directives meant to protect and maintain trade secrets. Implementation includes educating your employees about the protocols that need to be observed. These protocols may be somewhat challenging to establish in that an appropriate balance needs to be struck between your employees as valued members and concurrently as potential threats to the business. It is also important to keep in mind that these protocols serve as part of the good ‘story to tell’ about your internal security policies before enforcement bodies – such as courts and administrative agencies – which will expect that appropriate measures have been undertaken by the company in protecting its most valuable information.

Gerardi: Companies should involve financial, economic, technical and other experts early in the

pre-litigation and discovery phase to assure that they have the information they need to render fully defensible opinions.

Pooley: In light of the new US federal law, as well as the recent Trade Secret Directive issued by the

“Companies should involve financial, economic, technical and other experts early in the pre-litigation and discovery phase to assure that they have the information they need to render fully defensible opinions.”

*Christopher Gerardi,
FTI Consulting*

European Union, we recommend that companies immediately review their confidentiality agreements to ensure compliance. Second, they should revisit their external collaboration relationships – contracts with vendors, customers or other partners where confidential information is shared. If any of those involve parties in other countries, the relationship should be managed in a way to maximise the chance that any dispute will be heard in US courts, where meaningful remedies are available. This can involve contract terms, but also operations in which the foreign partner increases its contacts with this

country. Finally, they should take the occasion of the new statute to reconsider broadly their strategies involving exposure to trade secret litigation and their internal information protection systems.

Froud: Companies should close the stable door before the horse has bolted. The best cases to litigate are those in which the company has taken all reasonable steps to protect its trade secrets. Organisations should prepare for disaster rather than react when it strikes. Spending time to establish the appropriate layers of protection should pay off in the long run. In our experience, the very worst time to discover that protection is inadequate is when valuable business assets have been hijacked for

another's gain. Don't let someone else trade your secrets. Protect them.

Koris: Rather than focusing solely on the enforcement of trade secrets through litigation, the majority of effort should be on insuring the culture of the organisation is one directed toward leveraging value from its information and corresponding intellectual property in line with its investment expectations. Having a well thought out enforcement plan is an important consideration in the development of IP strategies. Likewise, preventing the loss of valuable information from cyber attacks requires a well-managed process which includes knowing what to protect. 