EISNERAMPER
ACCOUNTANTS & ADVISORS

EisnerAmper LLP
Accountants and Advisors

www.eisneramper.com

June 2016

Trends & Developments

TRANSFER PRICING

Applying Eminent Domain to IP Transfer Pricing

By Henric Adey

The concept of eminent domain dates back to biblical times, and is even highlighted in the U.S. Constitution's Fifth Amendment: "... nor shall private property be taken for public use, without just compensation."

The application of eminent domain has sparked recent interest with discussions about ownership and migration of intellectual property ("IP") under the Organisation for Economic Co-operation and Development ("OECD") base erosion and profit shifting ("BEPS") project. Tax planning strategies have allowed many multinationals to move IP off shore and into low-tax jurisdictions, allowing them to benefit substantially from lower tax rates. Researchers have long recognized that governments could eliminate dead-weight losses by making IP available to the public. The main concern is determining "just compensation" under the Fifth Amendment's "Takings Clause."

If just compensation under eminent domain is defined as the price paid to transfer IP, the threat of applying eminent domain creates a mechanism that eliminates dead-weight losses to society. IP owners must attest that the price chosen for such IP transfers meets the arm's-length standard, and such price mirrors the Takings Clause standard for determining just compensation. As such, a country's ability to take IP is a sufficient threat to deter tax avoidance through IP shifting.

Two sources could potentially provide U.S. states with the authority to take a privately owned patent. First, a government's eminent domain power may be extended to intellectual property, such as prescription drug patents. According to law professor Kevin Outterson, "[s]tates may exercise this power against pharmaceutical patents, just as they have always exercised eminent domain over real property."

Second, in *Florida Prepaid Postsecondary Education Expense Board v. College Savings Bank,* the U.S. Supreme Court held that states are generally immune from patent infringement if due process via just compensation is afforded to the patent owner. The Court indicated that a state's infringement of a patent is not by itself unconstitutional as long as some remedy is provided. In fact, "only where the State provides no remedy, or only inadequate remedies, to injured patent owners for its infringement of their patents could a deprivation of property without due process result." This provides states the ability to take privately held patents, provided just compensation is paid to patent owners.

IP proponents argue that patents, copyrights and trademarks should be called intellectual property in order to be covered by eminent domain protections. The Supreme Court has supported this argument, and states can take private property provided they pay just compensation.

Henric Adey is the Transfer Pricing Practice Leader at EisnerAmper. If you'd like more information, please contact Henric at 732.243.7272 or henric.adey@eisneramper.com.

Cyber Threats to Law Firms

By Hubert Klein and Jerry Ravi

The word "cybersecurity" is a buzzword that invokes fear in many people responsible for managing law firms these days. However, the proper reaction should be one of concern and action, not fear. Your organization has an opportunity to better protect itself from cybersecurity threats with proper planning, and in return reduce the threat of a data breach or, even worse, a lawsuit related to a data breach. Not being properly prepared for a data breach can lead to an economic loss, as well as reputational damage to a firm.

Many news reports and trade magazines indicate that hackers are increasingly targeting the legal profession for its data. Why? Because law firms' data files, both electronic and hard copy, contain a goldmine of sensitive and confidential information on both clients and firm assets. That information is valuable to criminals who traffic in stolen data files and personal information. In today's environment, cybercriminals are increasingly incentivized to secure content in order to make a profit. Like all crimes of opportunity, they look to the less risky and most vulnerable sources first. Those tend to be organizations that do not have secure, up-to-date data protection protocols. The cost to a law firm as a result of a data breach can run into the millions of dollars.

As technology has changed over the past decade, lawyers have been consistently using more electronic documents than they did in the past. Instead of FedEx and UPS packages containing hard copies of documents, they now use electronic data systems such as email, mobile devices, and other electronic communications to send 'soft copy' documents such as Word, Excel, Access and PDF data files, to communicate with clients and third parties. Many of those files are generated within the firm and are emailed out to various non-firm recipients. The reverse is also true: Many electronic data files containing sensitive information are received by law firms from clients and third parties as attachments. This happens on a regular basis these days. (Not much "send me a fax" anymore; it's much more frequently "email me the file or information, and I will put my electronic signature on it.") Regardless of the source or destination of data transmission, the raw data is generally stored on a firm server or with a cloud storage provider, as well as in backup files either on-site or off-site.

As a result, law firm IT and administrative professionals are increasingly under pressure to focus more resources in an effort to ensure that up-to-date cybersecurity and privacy standards are applied to their systems in order to control and manage information. At the same time, they are attempting to minimize their firms' risk and exposure to lawsuits for not properly protecting sensitive client and employee information.

Law firms are basically the same as any other company when it comes to countering cyber attacks and protecting their confidential and proprietary data. In today's environment, any organization in possession of sensitive data must have a security program that aligns with accepted best practices and standards. The typical response in many firms used to be "call IT," and then just hand off the responsibility to them and go back to work. However, time and the increasing pace of cybersecurity breaches have shown that this is not the best way to ensure against a cyber-threat. Cybersecurity is an enterprise business risk for all law firms, and includes everyone in the organization. That means professional staff, attorneys, firm management and support personnel need to be involved in understanding the risks, both reputational and business, from a liability standpoint. They must also buy in and be proactively involved in the establishment and enforcement procedures and protocols, and adhere to them.

How does the planning and development start? First and foremost, taking a risk-based approach will allow you to be the most effective at combatting cybersecurity risk. Begin by performing an overall cybersecurity risk

Cyber Threats to Law Firms *(continued)*

assessment. Establish a cross-organizational team comprised of professional staff, procurement staff, finance, human resources, communications, office management, and IT personnel. Make sure there is a "tone from the top" – firm leaders have to be on-board. The key areas to build out your security program area as follows:

- Identify the real risks:
  - o Develop a security strategy focused on business drivers and protecting high-value data.
  - o Define the organization's overall risk appetite.
  - o Identify the most important information and applications, where they reside, and who has/needs access.
  - o Assess the threat landscape and your security program maturity – model your real exposures.
- Protect what matters most:
  - o Balance the fundamentals with emerging threat and vulnerability management.
  - o Establish and rationalize access control models for applications and information.
  - o Protect key identities and roles that have access to the "crown jewels." Utilize 2-factor authentication methods for access to critical data.
- Sustain your security program:
  - o Get governance right – security is a board-level priority.
  - o Allow good security to drive compliance – not vice versa.
  - o Measure leading indicators to catch problems while they are still small.
  - o Accept manageable risks that improve performance.
  - o Know your weaknesses – and address them!
- Embed security in the business:
  - o Make security everyone's responsibility – it's a business problem, not just an IT problem.
  - o Align all aspects of security (information, privacy, physical and business continuity) with the business.
  - o Spend wisely in controls and technology – invest more in people and processes.
  - o Selectively consider outsourcing or co-sourcing operational security program areas.

After considering the above areas and performing a risk assessment, now is the time to ensure that you create and reinforce cybersecurity governance, policies and procedures, which ultimately translates to a continuous monitoring program.

- Develop a cybersecurity strategic plan (a 2- to 5-year plan) to include remediation protocols for activities identified in scans and penetration testing.
- Invest the resources necessary in cybersecurity technologies for data encryption, detection and monitoring.
- Identify and document cybersecurity controls – they need to be in writing.
- Establish policies and procedures for security configuration settings, access controls and logging.
- Conduct continuous training – without proper training, all your efforts will be in vain.
- Develop incident response, business continuity, and disaster recovery plans. Test those plans on an ongoing basis, at least once per year, to ensure you can respond and recover from a cybersecurity incident.
- Develop contractual cybersecurity requirements for outsourcing vendors, cloud providers, or other entities that connect to the firm's network.
- Conduct regular reviews of the security program, provide ongoing training, and update as necessary.

In the end, the best place for a cybercriminal to troll for data and content is on an unsecured or minimally secured system. While antivirus software is essential, it detects only a small percentage of system threats. New (and constantly emerging) malware programs and other

cybersoftware can penetrate poorly secured systems with relative ease. Specialized services that detect sophisticated attacks are generally required to properly protect an organization. Take a risk-based approach and continue to evaluate your people, processes/controls, and technology to ensure that your cybersecurity program is the most effective at your firm.

To determine if your systems are vulnerable to an attack or if your related policies and procedures are up to date, you should contact a cybersecurity specialist for assistance. Proper planning and implementation today can help your firm minimize its exposure and related legal liability in the event of a breach. As with everything else in running a practice, a cost/benefit analysis of the exposure to a cybersecurity breach is needed. However, while cost and resource allocation may be an issue, understanding and assessing any potential threat is needed in order to properly prioritize and allocate resources.

Hubert Klein is a partner in EisnerAmper's Forensic, Litigation and Valuation Services Group; while Jerry Ravi is a partner in our Consulting Services Group. Questions? Contact Hubert at 212.891.4011, hubert.klein@eisneramper.com or Jerry at 732.243.7590, jerry.ravi@eisneramper.com.

EMPLOYEE BENEFITS

IRS Expands Ability to Make Mid-Year Amendments to Safe-Harbor Retirement Plans

By Peter Alwardt, CPA

IRS Notice 2016-16 will help retirement plan sponsors comply with the safe-harbor plan notice rules for making mid-year changes. The Notice provides that a mid-year amendment to a safe-harbor plan (typically a 401(k) plan or a 403(b) plan) or to a safe-harbor notice will not violate the safe-harbor rules provided that 1) the plan satisfies the notice and election opportunity conditions, if applicable and 2) the mid-year change is not expressly prohibited in Notice 2016-16.

Background

Safe-harbor 401(k) plans are exempt from certain annual nondiscrimination testing (the actual deferral percentage test ("ADP") and the actual contribution percentage ("ACP") test). In exchange for this exemption, the safe-harbor rules require that the plan sponsor make certain specified minimum contributions, which are also fully (100%) vested when contributed. The plan sponsor is also required to provide a notice explaining the safe-harbor provisions to plan participants at least 30 days prior to the beginning of any plan year in which it intends to make safe-harbor contributions to the plan. Under prior IRS guidance, once plan sponsors provided the notice to participants, they could not amend their safe-harbor plan mid-year unless the plan sponsor was either operating at an economic loss or it had previously provided participants with a notice of the possibility to reduce or suspend safe-harbor employer contributions.

New Guidance Under Notice 2016-16

Under the Notice, a mid-year change is one of the following types of changes:

1. A change that is first effective during the plan year, but not effective as of the beginning of the plan year.

2. A change that is effective as of the beginning of the plan year, but not adopted until after the beginning of the plan year.

IRS Expands Ability to Make Mid-Year Amendments to Safe-Harbor Retirement Plans *(continued)*

If the mid-year change modifies the content of a plan's safe-harbor notice, then the plan sponsor must issue an updated safe-harbor notice not less than 30 days and not more than 90 days prior to the change becoming effective. Further, each employee that is required to receive a safe-harbor notice must be given a reasonable opportunity (including a reasonable period after the receipt of the updated notice) before the effective date of the mid-year change to make a change to the participant's salary deferral election. For this purpose a reasonable opportunity means at least 30 days.

Additionally, the Notice changes rules regarding mid-year changes to safe-harbor plans. Under prior guidance from IRS, any mid-year change was assumed to be prohibited unless expressly allowed under the guidance. Now, mid-year changes are assumed to be allowed unless specifically prohibited under IRS guidance. Accordingly, the Notice specifically prohibits the following mid-year changes:

1. Increasing an employee's required number of completed years of service to have a nonforfeitable right to the employee's account balance attributable to safe harbor contributions under a qualified automatic contribution arrangement ("QACA").
2. A reduction in the number of employees eligible to receive safe harbor contributions. This prohibition does not apply to an otherwise permissible change under either eligibility service crediting or entry date rules made for employees who are not currently eligible to receive safe harbor contributions under the plan.
3. Changing the type of safe harbor plan, for example, from a traditional safe harbor plan to a QACA 401(k) safe harbor plan.
4. Modifying or adding a formula for determining matching contributions or changing the plan's definition of compensation used to determine matching contributions if the change increases the amount of matching contributions or adds discretionary matching contributions. However, this prohibition does not apply to a plan making a mid-year change to allow discretionary matching contributions if:
    1. the change is adopted at least 3 months before the end of the plan year;
    2. is made retroactive for the entire plan year;
    3. and the plan sponsor gives an updated safe harbor notice and election opportunities to all participants.

Conclusion

The additional flexibility under the Notice should help make safe-harbor plans more attractive to some employers that previously were reluctant to adopt them. However, plan sponsors wishing to make mid-year changes to their plans must be vigilant with respect to the rules for updating the safe-harbor notice to plan participants, as well as seeking professional advice regarding any mid-year modifications they are contemplating making to their plan.

This article was previously released as an EisnerAmper Tax Alert.

Peter Alwardt is a tax partner specializing in employee benefits, tax and ERISA issues for domestic and international clients. For more information, please contact Peter at 212.891.6022 or, peter.alwardt@eisneramper.com.

EisnerAmper LLP is both proud and grateful to receive these accolades from our peers. They are a wonderful testament to our staff and their dedication to the clients and industries we serve.

Alt Credit Intelligence

Alt Credit Intelligence, an HFM Global publication, surveyed its audience of investors and fund managers and recognized EisnerAmper as the "Best Tax Advisor" at the U.S. Service Awards.

A.M. Best

For the fourth consecutive year, EisnerAmper has retained a top five ranking as one of the "Largest Property/Casualty Audit Firms." A.M. Best is regarded as one of the most trusted sources of insurance industry information.

Crain's New York

Crain's New York named EisnerAmper the "#1 Independent Accounting Firm in the New York Metro Area."

Hedgeweek

Hedgeweek, a leading hedge fund industry publication, voted EisnerAmper the "Best North American Accounting Firm," based on a survey of Hedgeweek's audience of investors, fund managers and industry service providers.

Institutional Investor

Institutional Investor magazine bestowed EisnerAmper with its Alpha Award for hedge fund accounting service providers. For three consecutive years EisnerAmper has been named leading accounting firm.

Private Asset Management

EisnerAmper swept the Forensic Accounting, Litigation & Valuation categories, winning first place in seven categories in the New Jersey Law Journal Best of 2015 reader survey.

The Legal Intelligencer

The Legal Intelligencer, the oldest law journal in the U.S., named EisnerAmper the leading firm in the Business Accounting, Forensic Accounting and Litigation Valuation categories in its Best of 2015 survey.