APRIL 15, 2021

Digital Due Diligence

Avoiding Risk + Succeeding in Digital

Presenters

James Devaney | Shook, Hardy & Bacon

Natalya Northrip | amazon

Jen Schroeder | Shook, Hardy & Bacon

ACC Association of Corporate Counsel CHICAGO

SHOOK HARDY & BACON

DIGITAL DUE DILIGENCE

“a collection of best practices around digital technology to minimize risk and maximize potential for success”

Intellectual Property

Strategic Patent Portfolio Creation

- Facilitates cross-licensing, freedom-to-operate, strategic partnerships
- Seek patents on innovation with strategic value, not necessarily tied to your product
- Implement procedures into workflows to capture all digital innovation occurring within your company. Anticipate innovation from all parts of your company
- Educate your employees and capture innovation early

Consider all aspects of your digital asset for IP protection

- E.g., Patenting; Trade Secret, and Defensive Publication and/or Open Source Software release

Patent–Product Portfolio Analyses

- Offensive or defensive assessments. Useful for licensing, monetizing, negotiating, avoiding litigation, and shaping strategy

Freedom-To-Operate (FTO) Diligence

- Assesses your company's exposure + Facilitates risk management + Enables patent design-around for commercialized products or services. DDD legal team works directly with your company's engineers or developers to modify aspects of your product or service to mitigate infringement risk

Patent–Product Portfolio Analyses

- Industrywide assessment of IP for particular technology areas to identify potential threats + opportunities for strategic acquisition/partnership or cross-licensing and portfolio development strategies. Useful when entering a new market.

Digital Technology Transactions

Due Diligence Investigation

- Identify Technology and IP Assets
- Ownership
- Software
- Domain Names and Social Media Accounts
- Data Privacy and Cybersecurity

Drafting Considerations

- Ownership of technology / IP
- Confidentiality obligations
- License terms (if applicable)
- Indemnification / risk allocation
- Representations and warranties
- Ancillary documents

Data Management + Cybersecurity

Privacy and Cybersecurity: Internal Processes

- Conduct data mapping
- Identify applicable requirements
- Implement privacy and cybersecurity frameworks

Data Retention: Best Practices

- Create data retention policy and retention schedule
- Implement policy and schedule

Data Incidents and Third-Party Risks

- Data held by the organization
- Data entrusted to a data provider

Regulatory Landscape

Transportation

NHTSA

Health

FDA, HHS

Financial

SEC, FDIC, CFTC

Communication

FTC, FCC

AI | Analytics | Apps + Software

Apps + software developed by your company

- Identify and document code and components subject to a license
- Determine governing license agreement (e.g., EULA, terms of use)
- Considerations when working with a vendor include Ownership (application program + source code + data | IP), Code escrow, Code auditing, Maintenance and Support, Distribution and Monetization (e.g., ads, user data)

Open Source Software (OSS)

- Understand OSS license types
- Create a corporate OSS policy

Artificial Intelligence: *Data + Models*

- Ownership and control (e.g., who owns the data, your company? users? a vendor?)
- IP protection
- Data governance + security
- Design defensively
- Create a corporate AI policy (Submission describes AI decision making + data used)

Takeaways:

- Digital technology carries unique legal risks across many different practice areas. Broad legal expertise in digital is crucial for managing these risk and maximizing potential for success. Engage experienced DDD counsel knowledgeable of the specific digital technology that can provide a comprehensive legal approach that considers your company's position and business objectives.
- IP strategy should be tailored to digital technology in order to protect your own innovations and to avoid infringing third-party IP rights.
- Digital technology transactions carry unique risks and thus require specific due diligence and drafting strategies.
- Data is a key aspect of digital technology, and cybersecurity and privacy policies and procedures are needed to manage risk and win trust.
- Regulatory landscape around digital technology is evolving.
- Processes around development of AI, apps, and other software should address license compliance, as well as security, ownership and control issues.

Contact

James Devaney

Partner

jdevaney@shb.com

Jen Schroeder

Partner

jschroeder@shb.com

HEALTH / SCIENCE / TECHNOLOGY / SHB.COM /

SHOOK
HARDY & BACON