KILPATRICK TOWNSEND

7 KEY TAKEAWAYS

Coexisting: Synergies and Tensions Among Open Source Software, Privacy, and Patents

Kilpatrick Townsend's Michael Pavento, Stephen Dew, and Tony Glosson, recently spoke on a panel at the firm's annual Kilpatrick Townsend Intellectual Property Seminar (KTIPS) on the topic of "Coexisting: Synergies and Tensions Among Open Source Software, Privacy, and Patents." The panel discussed the use and licensing of open source software and the patent and privacy law implications of doing so. Topics covered included the special considerations in open source software licensing. They also addressed data breaches involving open source software and breach response best practices.

Key takeaways include:

1

Open Source Software (OSS) is software for which source code is made available under a license. Licenses typically grant rights to study, change and redistribute to anyone and for any purpose. OSS enables companies to avoid having to "reinvent the wheel" and to focus on the value-added aspects of their product or service.

OSS licenses typically impose limitations on its use, therefore compliance with these terms is essential to avoiding copyright infringement and breach of contract claims. In general, licensee obligations occur on a *distribution* of the OSS or a modified version of the OSS. Common obligations include requiring attribution to the copyright holder and requiring any modified OSS be released in source code form.

2

3

Best practices include maintaining a formal written OSS usage policy, using a tracking system to review OSS usage requests, and verifying compliance prior to product shipment. A tracking system creates a record OSS in use which can later be used for license compliance or a security audit. Many licensee obligations occur on distribution.

When considering whether to contribute to an OSS project, consider the scope and purpose of the contribution and whether any proprietary IP is implicated. Consider the business value of the IP relative to the ecosystem benefits of the contribution. For instance, an OSS contribution implies a downstream IP license, yielding some proprietary IP rights. But on the other hand, a contribution may enable customers, vendors, and partners to build improved software for a company's platform.

4

5

Evaluate patent risks when using OSS. Many OSS contributors consider patents to be antithetical to open source. For instance, OSS licenses typically require, implicitly or sometimes explicitly, an OSS contributor to grant all downstream recipients a license to any and all of the contributor's patents that cover its contribution. Therefore, at a minimum, a company's own patent rights can be diminished if the company contributes to OSS. Some companies have made pledges to not assert patents against users of certain OSS, while some non-practicing entities have asserted patents against users of OSS.

Evaluate releases of company software for security vulnerability of any OSS components used. In some cases, vendors using OSS code components should be asked to provide cybersecurity and data privacy warranties as well as IP infringement. In this case, consider leveraging vulnerability databases such as NIST's National Vulnerability Database and MITRE's Common Vulnerabilities and Exposures ("CVE") database. Best practices include maintaining a "responsible disclosure" mechanism, such as an email through which security researchers can safely report vulnerabilities identified in company code. In the unfortunate event of a data breach, companies should carefully inventory their contractual breach notification obligations, in addition to regulatory and statutory obligations.

6

7

Blockchain-based technology is some of the fastest-growing open source developments. A Blockchain is decentralized, digital accounting ledger. Transactions are recorded in immutable blocks. Many Blockchain projects are open-source and therefore carry OSS obligations. But many applications of Blockchain technology carry both technical and social engineering risks that companies should ensure they understand.

For more information, please reach out to:
Michael Pavento: mpavento@kilpatricktownsend.com
Stephen Dew: sdew@kilpatricktownsend.com
Tony Glosson: tglosson@kilpatricktownsend.com

www.kilpatricktownsend.com