VENABLE® LLP

Articles

February 2014

Winter 2014 Federal Copyright and Trade Secret Legislation Update

AUTHORS

Armand J. (A.J.) Zottola

Robert F. Parr

RELATED PRACTICES

Intellectual Property

Copyrights and Licensing

Employee Mobility and Trade Secrets

RELATED INDUSTRIES

Cybersecurity

ARCHIVES

2014 2010 2006

2013 2009 2005

2012 2008 2004

2011 2007

Several bills under consideration in the 113th Congress would establish or significantly amend certain federal statutes related to the protection, enforcement, and exploitation of trade secrets or copyrights. Some legislation aims to establish a private right of action for trade secret theft under federal law or to prevent or deter trade secret theft through cyberattacks. Other bills are designed to repeal or leverage certain compulsory copyright license fees or to modify copyright laws relating to public performance rights and anticircumvention of technological access controls on consumer devices. If signed into law, these bills would have important implications on a wide range of interested parties, including performing artists, entertainment industry or content right stakeholders, and any business intent on exerting greater control over its trade secrets. Set forth below is a current summary of some of the more significant bills.

Trade Secrets

Recent developments in U.S. federal trade secret law spring from the **Economic Espionage Act of 1996** (EEA). While the EEA currently only provides for criminal prosecution, the **Future of American Innovation and Research Act (S. 1770)** (FAIR Act) would allow trade secret owners to bring civil actions for trade secret misappropriation against foreign defendants (or defendants located in the U.S. when the theft was intended to benefit a foreign person or entity). Designed primarily to target trade secret theft by or in favor of foreign actors or entities, under the FAIR Act, plaintiffs may seek damages, restitution, injunctive relief, punitive damages, and attorney's fees, and courts may seize items used to facilitate trade secret theft (*i.e.*, cell phones or computers). A similar version of the foregoing bill, the **Private Right of Action Against Theft of Trade Secrets Act of 2013 (H.R. 2466)** creates a private cause of action for trade secret theft against defendants located in the U.S. and further clarifies that claims for reverse engineering trade secrets are not actionable. The private right of action under these bills would presumably help companies that face trade secret theft involving international participants by facilitating multi-jurisdictional litigation involving witnesses and critical evidence located in another state or country. Under either bill, a private right of action would also allow companies to assert greater intellectual property rights over proprietary data, such as consumer data that has become a more important intangible asset to many businesses.

Several other pending bills addressing trade secret protection were introduced to prevent and deter trade secret theft resulting from cyber invasions or cyberattacks. These bills are largely reactionary to the recent wave of cyber intrusions, as best illustrated by a 2013 report that the Chinese military had hacked into the computers of many U.S. businesses in order to steal trade secrets. With respect to these bills, the **Cyber Economic Espionage Accountability Act (H.R. 2281)** (CEEAA) would permit the President of the U.S. to identify and penalize foreign officials that commit or aid cyberspying and trade secret theft through asset freezes, travel bans, visa revocations, and other punitive measures. Introduced only a month after the CEEAA in May of 2013, the **Deter Cyber Theft Act (S. 884)** would further require a watch list of offending nations to be created, and also mandate the President to direct U.S. Customs and Border Protection to bar imports from foreign countries named to a watch list.

Finally, several other trade secret protection bills look to strengthen trade secret protection under federal law by allowing the sharing of cyber threat information and by increasing or enhancing penalties for cyber criminals. For example, the **Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act (H.R. 1468)** creates a limited exemption from antitrust laws for the sharing of cyber threat information between private businesses, and aims to amend certain provisions of the Computer Fraud and Abuse Act to include criminal penalties for aggravated damage to certain critical infrastructure computers (*e.g.*, those that control chemicals or electricity). Along similar lines, the **Cyber Intelligence Sharing and Protection Act (H.R. 624)** (CISPA) is designed to permit information sharing about cybersecurity threats among government agencies and private companies. CISPA would allow the federal government to use cyber threat

information obtained from private companies for certain purposes including, without limitation, to investigate and prosecute cybersecurity crimes. In light of recent scrutiny over government initiatives to obtain and review data from companies, it is worth noting that CISPA has already drawn substantial criticism from privacy advocates and the White House and could have difficulty advancing.

Copyrights

Various bills under consideration in the copyright arena could lead to important changes in copyright law. Introduced in late 2013, the **Free Market Royalty Act (H.R. 3219)** (FMRA) would amend the U.S. Copyright Act (Copyright Act) to include a public performance right for any audio transmission of a sound recording. FMRA would then provide performing artists a right to collect royalties when their songs are broadcast over the radio or through comparable online services (*i.e.*, Pandora or Sirius XM). In addition, the FMRA would eliminate compulsory license rates for digital audio transmissions. Instead, copyright owners would be able to negotiate directly the terms of licenses to air their recordings, or opt to have such rates negotiated on their behalf by SoftExchange, Inc., a non-profit performing rights organization that collects royalties on behalf of sound recording copyright owners.

The Department of Commerce (DOC) is likewise exploring ways to update the Copyright Act and, in particular, to address the complexities associated with protecting copyrights on the Internet. The DOC recently received public comments on a green paper about copyright policy from major industry groups and other stakeholders on four hot-button issues: (i) statutory damages imposed on people caught illegally sharing content over the Internet; (ii) the sufficiency of the notice and take-down system set forth under the DMCA; (iii) whether the first-sale doctrine *(i.e.*, the right to resell without liability for copyright infringement) should be extended to digital products (*i.e.*, e-books and MP3 music files); and (iv) the uncertain legal status for musical remixes or "mashups." This process is designed to help the DOC develop policy recommendations on the foregoing issues which may include support for new legislation by Congress.

Other bills focus on changing the compulsory license fees required by the Copyright Act related to content distribution in the television and broadcasting industries. The **Next Generation Television Marketplace Act (H.R. 3720)** was introduced to repeal compulsory copyright license fees for certain transmissions of television programming by satellite carriers and also eliminates certain categories of remedies. Moreover, in an effort to give consumers more control over their satellite or cable services, the **Television Consumer Freedom Act of 2013 (S. 912)** aims to incentivize major television distributors covered by the statute (*i.e.*, Walt Disney Co., News Corp., and CBS) to let consumers purchase channels on an individual or "a la carte" basis. To this end, distributors that only offer channels in bundles or packages will not be permitted to pay the compulsory copyright license fee to distribute content. Instead, such distributors would have to negotiate with individual rights holders to distribute their content.

Another piece of legislation that has generated significant buzz relates to amending the Digital Millennium Copyright Act (DMCA). In 1998, Congress enacted the DMCA to address dramatic changes in the copyright landscape. Section 1201 of the DMCA prohibited consumers from bypassing or "unlocking" technical access controls on software or hardware devices to protect the underlying work from copyright infringement. The foregoing prohibition, however, is not absolute. The DMCA allows the Library of Congress (LOC) to exempt particular copyrighted works from the anticircumvention provisions of the DMCA for three-year periods.

In 2006, and again in 2010, the LOC exempted wireless mobile devices from the anticircumvention prohibition to let consumers reprogram their mobile devices in order to change wireless service providers. As a result, from 2006 to January of 2013, consumers could unlock their mobile devices without liability for copyright infringement. Nevertheless, in January of 2013 the LOC allowed the exemption to expire and therefore made cell phone unlocking illegal once again under Section 1201 of the DMCA.

Amid public outcry and political pressure, three bills were introduced in Congress by mid-2013 that narrowly focused on legalizing cell phone unlocking through different means. Of these, the **Unlocking Technology Act of 2013 (H.R. 1892)** (UTA) would amend Section 1201 of the DMCA and make it legal for consumers to unlock technical access controls on personally owned software or hardware devices as long as they do not commit copyright infringement once they have access to the underlying work. While "bootlegging" music and movies would remain illegal under the UTA, the bill would allow consumers to unlock cell phones, computers and other personal devices for purposes of repair, maintenance, and modification. UTA would further protect researchers, engineers, and companies that create, transmit, and otherwise make available the tools that facilitate the unlocking process.

The foregoing pending legislation may lead to significant changes in U.S. federal laws related to the protection, enforcement and exploitation of trade secrets and copyrights. Consequently, interested parties should monitor these bills to ensure they are fully aware of any developments that may affect their rights and obligations under U.S. federal law. This raft of current bills, however, could mark only the beginning of efforts to modify and expand U.S. federal trade secret and copyright laws. Stay tuned for further updates from Venable's **Intellectual Property** team on important developments in this area.