Cullen | Dykman

Is Ashley Madison abusing the Digital Millennium Copyright Act in the Wake of Hack?

September 1, 2015

In July, a group of hackers identifying themselves as the Impact Team took over the computer systems of Avid Life Media ("ALM"), the parent company of the adultery-oriented website Ashley Madison, threatening to release the names and personal information of over thirty million users of the site.

This data—which includes street addresses, email addresses, birthdates, and phone numbers—was released on the "dark web" in August, and was accessible only to users of the Tor browser. Soon after, numerous websites sprang up that provided search engines for the data—providing an easy way for an individual to check to see if his or her spouse had signed up with the Ashley Madison site.

ALM quickly began sending Digital Millennium Copyright Act ("DMCA") notices to many of these search engine sites, claiming to own a copyright in the stolen Ashley Madison data. The DMCA was passed in 1998, to protect against copyright infringement on the Internet and to provide a "safe harbor" for websites that act quickly to remove posted material that is allegedly copyrighted.

Under the DMCA, the owner of copyrighted material that has been posted to a site without permission can send what is called a "takedown" notice to that site, containing certain information—including an identification of the subject work, contact information of the individual or entity sending the notice, and a signed statement (under penalties of perjury) that the complaining party is the owner of the allegedly copyrighted material or is authorized to act on behalf of the owner.

Once a website owner receives a takedown notice, to avoid liability under the DMCA "safe harbor" provisions, the material must promptly be removed from the site and the site owner must notify the user who posted the content. The user then has the option of sending a counter-notice to the site, asserting that the removal was not proper. If such a notice is received, the site must notify the sender of the original takedown notice, who then has 10-14 days to file a lawsuit. If no suit is filed, the site may re-post the content.

The DMCA, however, only allows for the protection of *copyrightable* material. In *Feist Publications v. Rural Telephone Service Co.*, 499 U.S. 340 (1990), the Supreme Court held that simple listings of facts—such as an alphabetical listing of individuals in the phone book—cannot be copyrighted because such information lacks the minimum level of creativity necessary for protection under the law. It is this type of information—listings of Ashley Madison user information—that ALM seeks to remove from the Internet under the DMCA.

Some sites, upon receipt of the DMCA takedown notice from ALM, have removed the data, most likely to avoid potential costly litigation. However, other sites have refused on the grounds that ALM's notice is improper because ALM does not own a copyright in the leaked material. The only way ALM could potentially have copyright in such data is if there was some sort of creative compilation of the material, rendering it an "original work." However, this does not seem to be the case here. The majority of the leaked data is lists of names and other information, precisely the kind of material the Supreme Court has held is not entitled to copyright protection.

ALM is likely using the DMCA takedown notice in an attempt to mitigate the onslaught of legal action that is likely to follow in the aftermath of the hack, which reportedly contains information of individuals living in all but three zip codes in the United States. However, the DMCA provides that any individual who "knowingly materially misrepresents" that an activity is infringing may be liable for monetary damages, including costs and attorneys' fees incurred by the alleged infringer.

It is possible that ALM could face some kind of penalty if it is eventually found to have abused the DMCA by sending out numerous takedown notices for content in which it does not own a copyright. These penalties, however, are likely to come only after the years and years of litigation likely to arise from the massive privacy breach.

If your institution has questions or concerns about this topic and you would like further information, please email Karen I. Levin at klevin@cullenanddykman.com or Ariel E. Ronneburger at aronneburger@cullenanddykman.com.