Disclosure Leaks: Can Companies Take Legal Action?

It's not my area of expertise, but let's take a little detour into the realm of cyberlaw and tort law (IP/IT and tort attorneys feel free to chime in at any time).

The question came up: what, if anything, can a company do if material information, such as an earnings release, is obtained from an unpublished url and disseminated without the company's permission?

This can be a complicated query and does not fall squarely into one area of law, but there are a couple of different legal remedies that may be available:

Copyright Infringement

For starters, a company's disclosures may qualify for protection under the U.S. federal copyright laws, which, among other things, afford a copyright owner the exclusive right to reproduce, distribute and publicly display their work. To be copyrightable under the Copyright Act of 1976 a work must be:

- original – independently created (as opposed to copied from another work);
- possess at least a minimal degree of creativity – factual information is not copyrightable, but it is possible for a compilation of factual information to be copyrightable if the facts are arranged in a creative way; and
- fixed in any tangible medium – this includes any electronically readable format (*e.g.*, a work stored in a computer's memory).

Trespass to Chattel

Trespass to chattel is a common law intentional tort (a civil wrong) that protects personal property, including intangible property, from wrongful interference. Trespass to chattel in the digital context is still an evolving doctrine, but generally proving a claim requires a company to establish that there was an intentional interference with its possessory interest in personal property (the chattel) either by disposition of the property or by using or intermeddling with it. However, because trespass to chattel is a common law cause of action—one that has evolved through case law rather than governed by statutory or administrative laws—the elements of a claim can vary slightly from state to state and between state and federal jurisdictions. For example, some states require proof of damages to a company's servers or other systems in order to establish a claim, while others will accept wrongful interference without damages as sufficient.

The Computer Fraud and Abuse Act

As originally enacted, the Computer Fraud and Abuse Act of 1986 (CFAA) was a criminal statute intended to address crimes related to government computers and the computers of certain financial institutions. The statute was subsequently amended to provide for civil remedies for any person who suffers damages or losses in excess of $5,000 in any one year because of a violation covered by the CFAA.

A civil CFAA claim may be brought under any one of several different categories, including:

- intentionally accessing a computer without authorization, or in a manner that exceeds authorization, and thereby obtaining information; or
- intentionally accessing a computer without authorization and thereby causing damages or a loss.

Courts interpret the phrases "without authorization" and "exceeds authorization" differently, with some finding that a person who is authorized to access a computer nevertheless exceeds that authorization when intending to use the information obtained for an improper purpose, and others finding that a person must not be authorized to access a computer before the provisions of the CFAA will apply. In the context of websites, many courts have found that accessing a site indirectly, by use of a spider or robot program, falls within the category of access without authorization or in excess of authorization if that access is in violation of a sites terms of service (more on this in a moment). Courts also differ in their interpretation of what constitutes "damages or a loss" for purposes of a CFAA claim.

Violations of the Terms of Service

Most, if not all, company websites include a link to the "Terms of Service", "Terms of Use", "User Agreement" or the like, which specify the terms and conditions upon which the site may be accessed. Courts have generally found terms of service to be binding and enforceable on a site's users, even if they are never read or the site is accessed indirectly, by a spider or robot program, provided the terms are, or a link to the terms is, clearly displayed. Terms of service can be drafted to expressly prohibit certain uses or types access. For example, many terms of service specify that a site's content may be used only for personal and non-commercial purposes, and may not be copied or distributed without permission. Some terms of service also prohibit access by spider or robot programs.

If your company is moving, or thinking about moving, to web disclosure you should review your terms of service to ensure that they reflect what is and is not acceptable use and access of your site in light of your disclosure and investor relations practices.

Just Because You Can Doesn't Always Mean You Should

Then there is the question: should a company have to resort to legal remedies when material information is obtained from an unpublished url and disseminated without the company's permission?

As companies increasingly move to web disclosure these sorts of mistakes are likely to occur from time to time, and, of course, companies are absolutely responsible for and should fully understand the web disclosure technologies they use and have disclosure controls and procedures in place to protect their material information. At the same time, however, are those who are finding and distributing these mistakes acting like responsible market participants? They are certainly garnering attention and the fact that a mistake was made may very well be newsworthy, but are there other, less disruptive ways of handling a situation like this, and, if not, should they refrain from distributing the information at all? Just because you can do something, doesn't always mean that you should.