Find Waldo in Cyberspace

Forensic detective work meets digital media IP litigation

By Chris K. Ridder / Ridder, Costa & Johnstone LLP & Michael Purcell / Inventus, LLC

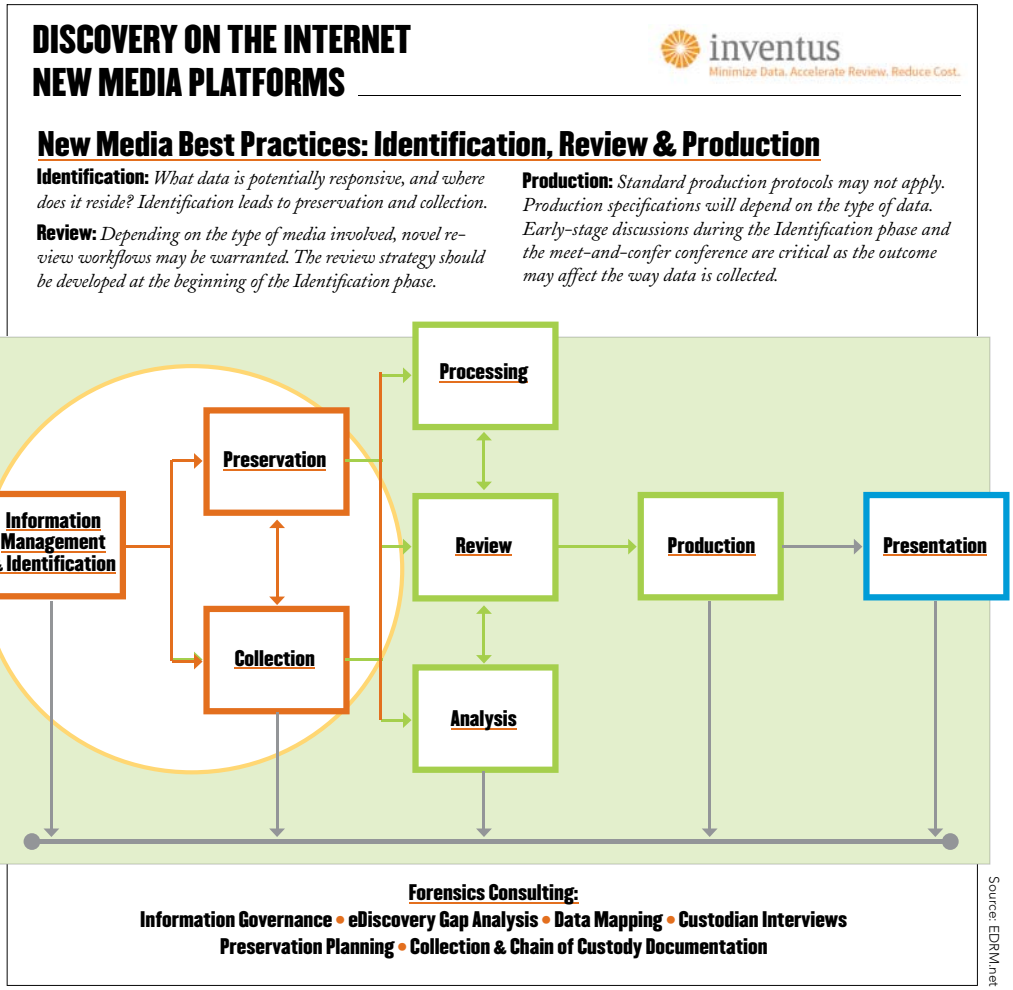
You don't have to have been around in the days of TV with only 13 channels and news cycles measured in days rather than minutes to have noticed the rapid and wide-ranging expansion of digital media in recent years – from the continued development of blogging and other forms of citizen journalism to the proliferation of social media platforms of every kind. The policy decisions that triggered the consolidation of old media have not yet been made for new media, which is being further fueled by amateur-produced digitally driven content. The result is a staggering variety of content and content delivery mechanisms – long form and short form, online-only and hybrid, image-driven and text-based, scripted and interactive, free and pay, archived and streaming, regulated and unregulated.

Growing Pains

Pioneers never have it easy. They're navigating uncharted waters. However, in the digital media age, the waters aren't merely uncharted, they're roiling with powerful currents created by an endless flow of commercial and consumer transactions and social interactions being conducted within a diverse ecosystem of formats, operating systems, browsers, platforms and devices, unbound by sovereign borders. This sea change has given rise not only to more media-related disputes, but to a dispute environment that is markedly more diverse, novel and complex than was the case with traditional media. Companies today struggle with data breaches, computer intrusions, and a rapidly evolving intellectual property landscape.

Copyright infringement claims continue to be a hot area. Like mushrooms after rain, they've been springing up from the different types of technology that are enabling content to be used and distributed in new ways. In U.S. law, copyright liability comes in two main forms, primary or direct, and secondary. Direct liability attaches to the actual infringer of the copyright in question, whether by copying without authorization or by violating any of the other rights that copyright owners possess. In recent years, the fair use doctrine has been strengthened by a number of court cases, making direct liability in some situations more challenging to establish. But most Internet providers and intermediaries are concerned primarily with secondary liability, a set of doctrines that is undergoing rapid change, partially in response to the challenges posed by new technology.

To what extent is a platform that hosts content liable for the content that appears on the platform? And what sorts of standards are intermediaries held to in different contexts?



Copyright Infringement

In the case of alleged copyright infringement, an online intermediary can be liable for "contributory infringement" if it had (i) actual or constructive knowledge of the direct infringement and (ii) made a material contribution to the direct infringement; or for "vicarious infringement" if it (i) benefitted financially from the direct infringement and (ii) had both the right and ability to supervise the direct infringer, a concept rooted in agency law. And there are key cases interpreting "material contribution," "ability to supervise" and other such terms, some of which have gone up to the Supreme Court. In a 2005 opinion concerning peer-to-peer file sharing, *MGM v. Grokster*, the Supreme Court recognized a third form of secondary liability: intentionally inducing or encouraging direct infringement.

Linked Content

The ability to display content from one site within another is part of the design of the Web's hypertext medium. While it is copyright infringement to make copies of a work for which you have no license, there is no infringement when you provide a simple text link within an HTML document that points to the location of the original image or file.

The use of a linked object, often an image, from one site by a Web page belonging to a second site – also known as hotlinking, leeching, piggybacking, direct linking or offsite image grabs – has been the source of a lot of controversy and sometimes liability.

Ridder, Costa & Johnstone handled a case for a client that operated a Web forum, the content for which was robotically aggregated, managed and optimized. The robot combed RSS feeds for relevant content and posted inline links. So it appeared as if the content was on the forum, but in fact it was just linked. Somebody alleged that one of those hyperlinks was infringing.

In *Perfect 10, Inc. v. Amazon.com, Inc.* – after the U.S. District Court, Central District of California, ruled that Google Inc.'s thumbnail images were infringing, but its hyperlinks to infringing sites were not infringing – Google appealed the injunction against its use of the thumbnails, and adult entertainment site Perfect 10 appealed the decision on the hyperlinks. The Ninth Circuit upheld the district court's decision that the hyperlinks did not infringe on Perfect 10's copyright, and that the infringing websites existed before Google, would continue to exist without Google, and thus Google was not a contributory infringer. The court also noted that Google had no control over infringing sites and could not shut them down, so any profits it may or may not have extracted from users visiting those sites did not constitute vicarious infringement.

The court also agreed that including an inline link is not the same as hosting the material yourself. So in the case of framing, while it may "appear" that Google was hosting infringing material, it was only hosting a link to the material that the browser interpreted should appear in a certain way. In another blow to Perfect 10, the Ninth Circuit held that the caching of thumbnail images was a fair use, given their small size relative to the original images and their transformative purpose as search tools.

Where's Waldo?

One of the big issues that we face in litigating Internet-oriented cases is identifying the malefactor. On the Internet, as any user knows, one can post content anonymously or pseudonymously. You can be a member of multiple sites and have a different username for each one, none of which is your real or legal name. The question that often arises in cases where someone posted defamatory content or confidential information on the Internet is "Who is that someone?" A client will come to us and say, "This content is defamatory or infringing, or somebody is hacking my computer," and our first response is, "How are we going to find these people?"

Usually it involves sending a subpoena to the host of the site with the offending content. In response to the subpoena, we will normally receive an Internet Protocol (IP) address. We then will take the IP address and, typically, subpoena the Internet service provider who owns it, requesting that it tell us which of its subscribers was using the IP address at the time the content was posted. Now we have the address of somebody's house, and the question becomes: Is that enough to prove that a "particular" individual was involved? Maybe there are four individuals living in the house. Maybe the house has an open WiFi and the neighbors use it. How do we know who the person was?

Having experts who can steer clear of technobabble is critical in a jury trial.

A lot of times we identify people with old-fashioned detective work. We call up the house and ask point blank about the content. But often, getting that proof may require calling a firm like Inventus and saying, "We need forensic evidence of who was using the computer at that time."

Digital Trade Secrecy

Theft of trade secrets has become more prevalent in the digital age. As in the past, it usually involves departing employees taking work product or confidential information with them when they leave. But unlike the past, the vast amount of digital information to which they had access creates the potential for massive data theft, and raises forensic questions as to what data was copied at what time.

There are also novel legal issues. In one case, the trade secrets primarily consisted of open source software, which begged the question how something "open source" could be considered a "trade secret." Was it the employee's disclosure of *which* open source software the company had on its servers that constituted the theft? Or did the employer's modifications to the software, however insignificant or inconsequential, confer trade secret status upon it, or a copyright in it? Big companies struggle with open source issues all the time. While it doesn't always result in litigation, it can complicate one's copyright picture enough that you just have to be cognizant of it. A lot of copyright complexity can be caused by improperly managing one's open source vs. closed source software.

Turning Your Experts into Strategic Partners

Usually, when a lawyer is dealing with technical evidence and technical concepts in litigation, there's an expert involved, and sometimes more than one. Like many things in law, it's a giant puzzle, and all the pieces come together. The data collection strategy is driven by the lawyer's theory of the case, which is driven by an understanding of the technology, which is informed by an expert. A lawyer who concentrates in this area has considerable technical fluency, but partnering with a service provider like Inventus makes things a lot easier, from developing a theory of the case to helping the lawyer explain the technicalities to the court. And of course one of the consultant's greatest values is as an expert witness in the courtroom, talking directly to the judge and jury. Having good experts who can speak to laypeople and steer clear of technobabble is critical in a jury trial, especially in federal court, where a lot of these cases are venued. In the Northern District of California, judges deal with technology every day, while in other jurisdictions, there may be less familiarity. In addition to the guidance of experts, many federal judges have clerks who are millennials and likely to have some fluency with the Internet and related technical concepts.

Chris K. Ridder
Partner at Ridder, Costa & Johnstone LLP.
chris@rcjlawgroup.com

Michael Purcell
Vice president of Strategic Solutions, Inventus, LLC.
mpurcell@inventus.com