Supplement to the Los Angeles and San Francisco
Daily Journal
APRIL 9, 2014

TOP INTELLECTUAL PROPERTY ATTORNEYS OF 2014

The most fascinating, and challenging, aspect of naming the intellectual property attorneys in California is the extraordinary variety of their achievements. While they share the same practice area, the lawyers — chosen from hundreds of nominations, along with a few staff selections — range from patent specialists who try cases before the U.S. International Trade Commission to Internet experts who fight the creators of malicious software "botnets."

To qualify for the list, an attorney must be based in California, even if much of his or her work is done elsewhere, whether it's the ITC in Washington, D.C., the patent office in Virginia, or district courts in Delaware, Texas and other states. Their focus must be intellectual property, as opposed to general litigators who often handle such work.

The attorneys chosen for the list have helped to advance technological innovation and change the law during the past year, handling work critical to the future of the entertainment, medical and technology industries.

It's an increasingly difficult group to choose, but the impressive and diverse array of talent from across California is testimony to the state's leadership in intellectual property law.

—The Editors

TOP LITIGATORS OF INTELLECTUAL PROPERTY

GABRIEL M. RAMSEY

FIRM: ORRICK, HERRINGTON & SUTCLIFFE LLP

CITY MENLO PARK

SPECIALTIES TRADE SECRETS, PATENT, COPYRIGHT

Ramsey devotes much of his time to chasing down elusive cyber bad guys and malicious "botnets" wreaking havoc on the Internet. Most of the time he doesn't know who he's up against, but that's what makes his work stimulating.

"If you slip up, the bad guys have all kinds of means to get control back," he said. "It's exciting and interesting and tough to do."

One of his biggest victories came late last year. In November, Ramsey filed a takedown action to turn off the primary command and control of a click fraud botnet called ZeroAccess that targeted Microsoft Corp. and its customers.

The botnet had enslaved more than 2 million PCs with malicious software in an elaborate and lucrative scheme to defraud online advertisers. *Microsoft Corp. v. John Doe 1 et al*, 13-1014 (W.D. Tx., filed Nov. 25, 2013).

Ramsey and his team worked closely with Europol, which quickly responded to the new infrastructure that the defendants tried to put in place after their original infrastructure was cut off.

That put enormous pressure on the defendants and suddenly they were very vulnerable to being identified.

In the end, they pushed a code update that disabled all the malware on the infected computers and included the repeated text string "WHITE FLAG" within the code, signaling their surrender.

"At first we were skeptical and thought it was a game," he said. "But they never came back. I think they decided it was time to stop."

Ramsey says it's the practical issues that keep him intrigued. Being anonymous on the Internet is easy, making it difficult to figure out who is behind malware or millions of spam emails across the globe.

"Working with investigators to put bread crumbs together and get to a person is kind of like the Holy Grail," he said. "It's really hard to do, but when you're successful it's really fulfilling."

— Sarah Parvini