IRWIN IP
INTELLECTUAL PROPERTY LITIGATION

IP CASE OF THE WEEK

Slip-and-Fall into *Enfish* Harbor Cuts Wonderland Tour Short

SRI Network Security Patent Survives *Alice* Step One

By: Iftekhar Zaim and Jared Hedman | April 3, 2019

On March 20, 2019, a divided panel of the Federal Circuit Court of Appeals held, among other things, that two network security patents asserted by SRI International, Inc. ("SRI") against Cisco Systems, Inc. ("Cisco") were not directed towards an abstract idea, thus affirming the District of Delaware's denial of summary judgment for invalidity. *SRI Int'l., Inc. v. Cisco Sys., Inc.*, Case No. 2017-2223, ___ F.3d ___, 2019 WL 1271160, at *3–5 (Fed. Cir. 2019).

The Court's decision is the latest in a line of recent cases rebuffing patentability challenges at Step One of the two-step test for patent-eligible subject matter set forth in the Supreme Court's landmark 2014 decision in *Alice Corp. v. CLS Bank Int'l.* 573 U.S. 208. *SRI* follows in the footsteps of the Federal Circuit's 2016 opinion in *Enfish, LLC v. Microsoft Corp.*, and seems to further define the safe harbor for patent claims directed towards improvements of a computerized system's functionality.[1]

SRI's asserted patents relate to a cyber-defense technology that is designed to improve enterprise-scale network security systems by placing a number monitors throughout the network's various domains to analyze any of myriad aspects or metrics of network traffic to identify suspicious behavior. Their reports of suspicious activity are then sent to a hierarchical monitor for further analysis. In practical terms, the method could enable the monitoring system to 'see the big picture' and perform centralized threat analysis. Such a system could, e.g., detect coordinated multi-vector attacks whose telltale indicia, if analyzed locally and in isolation, may not trigger a flag or response.

The majority repeatedly emphasizes that the claims of the SRI patents are directed to improving the functionality of a network itself, relying upon the patent's teaching of a specific technique that departed from the conventional localized method of network threat detection, and that a human could not perform that analysis. *Id.* at *4–5. The dissent, in stark contrast, found the claims to be "result-focused, functional claims" of the type that "frequently run afoul of *Alice.*" *Id.*, at *12 (citing *Elec. Power Grp.,* 830 F.3d 1350 (Fed. Cir. 2016))(holding that an electrical power grid monitoring system was directed towards an abstract idea). The majority distinguished *Electric Power Group* on the basis that the claims there used a computer as a tool to solve power grid problems, finding SRI's claims analogous to those in *DDR Holdings* insofar as they improved the network system itself. *Id.*

At its core, the Court appears to be emphasizing an essential distinction that has proven elusive to practitioners and courts analyzing computer technology patents: whether claims are directed to (1) an ineligible abstract idea; or (2) a patentable reasonably specific improvement to technology that, by its nature, exists in an abstract or virtual realm. SRI's claims do appear a close call, and a divided panel held them to be the latter. Perhaps, in *SRI* the Federal Circuit may have marked a limit of the *Enfish* safe harbor (at least until the next opinion in this ever changing area of law).

---

[1] For a more detailed background on *Alice*, *Enfish*, and the surrounding body of law, we would suggest taking a look at our prior article ("*Enfish* Secured; *Alice* Abridged") on the Federal Circuit's decision in *Ancora Techs. v. HTC America*.