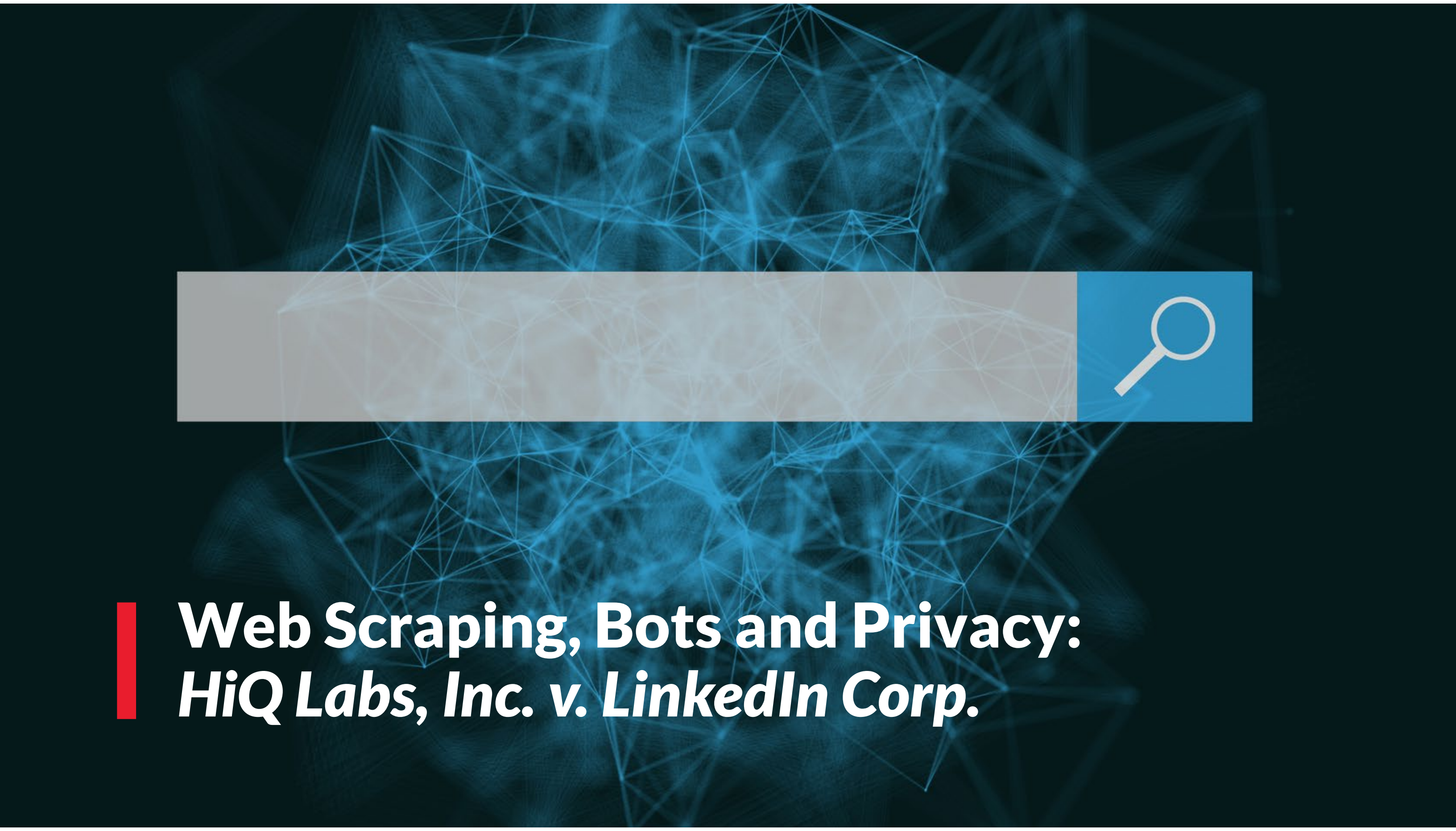

# Web Scraping, Bots and Privacy: *HiQ Labs, Inc. v. LinkedIn Corp.*

You're probably already familiar with LinkedIn®. It's a popular networking site that's designed for professionals across the entire spectrum of industries, from C-suite executives to gigging musicians. The site allows individuals to upload personal information, sort of like a digital resume, which can then be searched by employers, colleagues and friends.

That means LinkedIn is chock-full of data, ranging anywhere from a person's employment history to the name of their high school mascot. That trove of information can be a veritable goldmine for companies who specialize in data analytics.

One analytics company in particular, hiQ Labs, thought the same thing.

## THE ROLE OF DATA ANALYTICS

The science of analytics is creeping into practically every industry. By analyzing massive data sets, a savvy individual can (among other things) spot trends, predict the future and refine efficiencies. And that's precisely what hiQ Labs and its customers wanted to do.

It realized that the data within LinkedIn could be used to help business leadership gain insight into their employee's habits, skills and preferences. HR managers could use that information to improve employee retention, increase morale, better train personnel, enhance recruiting efforts and more.

Best of all, since the LinkedIn information was public and freely shared by the participants, there wouldn't be any negative implications in harvesting the data.

Or so hiQ thought.

## THE RISE OF THE BOTS

LinkedIn had a lot of data. Far too much for manual transcription. Aside from being an absolutely dreadful job, it simply wouldn't be possible for a human being (or an army of human beings) to review every profile, and collect and sort the data they'd find.

So hiQ built a bot. In this context, a "bot" is a bit of software code that scans and collects data on webpages—all automatically and in a fraction of the time it would've taken a human. It's a common, typically innocuous process that's know known as "scraping" a website for information.

> *Bots can come in a wide range of flavors—some good and some bad. For instance, malicious bots can spread disinformation on social media sites, while chatbots can simply help with customer service.*

Through scraping, hiQ now had a mammoth trove of personal information that it could package and parse out to interested (read: paying) parties.

And everyone was happy.

## THE LEGAL VOLLEY

Well, not exactly everyone—LinkedIn didn't like the idea of a data analytics company scraping its site. So, it began blocking the bots electronically and sent hiQ a cease and desist letter, citing potential violations in the Computer Fraud and Abuse Act. LinkedIn also asserted that hiQ had violated the website's terms of service.

HiQ fired back with a lawsuit, saying LinkedIn was engaging in unfair business practices. Without being able to access the information from LinkedIn, the company simply could not operate, which amounted to tortious interference. The information hiQ was scraping, after all, was given willingly by the members of LinkedIn and publicly available for anyone to access—the company was just accessing the information on a macro scale.

The resulting case, *HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019)*, involved a confluence of several issues, including data security, antitrust laws and the distinction between private and public information.

The court's ruling was poised to be significant.

All told, the court decided that, since the information hiQ scraped was public, the CFAA didn't really apply. That also meant that the bot issue was irrelevant—obtaining the public data was legal, regardless of the specific methods used to acquire it.

In fact, the court brought up the public nature of the information specifically. It asserted that individuals creating LinkedIn profiles would likely be aware that the information they're posting would be public.

> *Run a business and concerned about your role in protecting private data? Read this.*

## AFTERMATH

Topics like data collection, online privacy, biometrics and similar subjects will continue to be hot button issues for years to come. And, the infancy of the internet relative to other media means that courts can struggle to find applicable precedent.

Moreover, there hasn't been a large scale adoption of federal laws or regulations regarding online data protection. But codes and statues may not even matter in situations like this—given the speed in which technology evolves, it's fair to say that legislation will always lag behind, which means the courts are often relied upon for guidance.

That's why the hiQ case drew so much attention from the tech and legal sectors. It offered a glimpse into how the courts would treat the third-party use of public online information, while exploring the limits of the Computer Fraud and Abuse Act.

### About LexisNexis® Legal & Professional

LexisNexis Legal & Professional is a leading global provider of content and technology solutions that enable professionals in legal, corporate, tax, government, academic and non-profit organizations to make informed decisions and achieve better business outcomes. As a digital pioneer, the company was the first to bring legal and business information online with its Lexis® and Nexis® services. Today, LexisNexis Legal & Professional harnesses leading-edge technology and world-class content to help professionals work in faster, easier and more effective ways. Through close collaboration with its customers, the company ensures organizations can leverage its solutions to reduce risk, improve productivity, increase profitability and grow their business. LexisNexis Legal & Professional, which serves customers in more than 175 countries with 10,000 employees worldwide, is part of RELX, a world-leading provider of information and analytics for professional and business customers across industries.