LinkedIn data-scraping case highlights calls for SCOTUS review of computer fraud law

Alison Frankel

August 15, 2017

(Reuters) - Is it time for the U.S. Supreme Court to decide how the 1986 Computer Fraud and Abuse Act - a law enacted before ordinary people could even access computer networks – applies in the Internet age?

This fall, the justices will consider requests to review that overarching question in two very different cases from the 9th U.S. Circuit Court of Appeals, Power Ventures v. Facebook and Nosal v. United States. And if the justices need proof of the urgency of the issue, they got it Monday in a decision from U.S. District Judge **Edward Chen**of San Francisco.

Judge Chen granted a preliminary injunction to the data analytics startup hiQ, which relies on access to the public profiles of LinkedIn members to create products it sells to employers like eBay and GoDaddy. LinkedIn had sent hiQ a cease and desist letter in May, cutting off the data miner's access and threatening action under the CFAA if hiQ tried to circumvent the block. HiQ sued in June.

To ruthlessly simplify the two sides' arguments: LinkedIn claimed it has a right to protect the privacy of its users by blocking users that violate its terms of service, just as a public library might cut off borrowing privileges for someone who used a fake ID or refused to return a book. HiQ countered that it never trespassed but only accessed LinkedIn data available to the entire world, like any onlooker in a public square. Both sides brought in legal poohbahs - former U.S. Solicitor General **Donald Verrilli** of **Munger Tolles & Olson** for LinkedIn; Harvard prof **Laurence Tribe** and **Farella Braun & Martel** for hiQ - for a preliminary injunction hearing last month.

Judge Chen agreed in Monday's opinion that it makes sense to draw an analogy between the CFAA and physical trespass laws. The CFAA was enacted to deter computer hackers, who are literally computer trespassers. The tough part of interpreting the statute, however, is determining when a user actually is trespassing. Relying heavily on the reasoning of George Washington University law professor **Orin Kerr** in a 2016 paper, Norms of Computer Trespass, Judge Chen concluded that the key consideration is whether the computer owner has imposed a virtual lock on its doors, in the form of passwords or other software restricting public access.

Under Judge Chen's analysis, a user could be considered unauthorized, in the statutory language of the CFAA, if it tampered with those virtual locks or stole a key to open them. But if the computer owner has left its doors open, Judge Chen said, users are authorized to pass through them.

"The court intuitively understands that where an individual does not have permission to enter, he would be trespassing if he did so," the judge explained. "Even if the door is open to the public for business, the shop owner may impose limits to the manner and scope of access (e.g., by restricting access to a storage or employees-only area). But if a business displayed a sign in its storefront window visible to all on a public street and sidewalk, it could not ban an individual from looking at the sign and subject such person to trespass for violating such a ban. LinkedIn, here, essentially seeks to prohibit hiQ from viewing a sign publicly visible to all."

Judge Chen has spent a lot of time thinking about the Computer Fraud and Abuse Act – he presided over the 2013 CFAA prosecution of David Nosal, who was accused of supervising colleagues who used friends' login credentials to access the computer systems of their former employer, the executive recruiter Korn Ferry. His conclusion in the LinkedIn case is notable for its deep understanding of the law.

But it's even more notable that the judge is worried about whether businesses like LinkedIn can take advantage of the CFAA for their own purposes, "a result that Congress could not have intended when it enacted the CFAA over three decades ago," the judge wrote. Under LinkedIn's formulation of the CFAA, he said, website owners could cut off access based on users' race or gender. Political campaigns could block rival campaigns or unsympathetic news organizations. Companies could hobble competitors that sought to use public information about their products or pricing.

In short, Judge Chen wrote, "a broad reading of the CFAA could stifle the dynamic evolution and incremental development of state and local laws addressing the delicate balance between open access to information and privacy – all in the name of a federal statute enacted in 1984 before the advent of the World Wide Web." (The CFAA was enacted in 1986, as an amendment to a 1984 computer fraud law that was part of an omnibus anti-crime bill.)

Judge Chen's fear of CFAA abuse brings me to the Power Ventures and Nosal petitions for Supreme Court review. In both of those cases, the 9th Circuit found users to have violated the computer fraud statute. Nosal, as I mentioned, was convicted for unauthorized access to the website of his former employer. Power Ventures, a social media site, was found to be in breach of the CFAA when it used its members' login credentials to access Facebook after Facebook sent Power Ventures a cease-and-desist letter.

Power Ventures, represented at the Supreme Court by **Hughes Hubbard & Reed**, contends it was authorized because its members supplied their Facebook credentials. Facebook, represented by **Orrick Herrington & Sutcliffe**, argued that there's no need for the justices to hop into a case with idiosyncratic facts when the federal circuits aren't split. Briefing in that case is complete. Nosal, who is represented by **Hogan Lovells**, presents a similar question of whether defendants can be criminally liable under the CFAA when they have obtained permission (and login

credentials) from an account holder authorized to access a computer but have not received authorization from the computer owner. The Justice Department's response to Nosal's petition for Supreme Court review is due on Sept. 5.

Amicus briefs in the two cases, from the Cato Institute in Power Ventures and from the Electronic Frontier Foundation in Nosal, rang the same alarm bells as Judge Chen did in Monday's hiQ case. Congress never intended the CFAA to be an all-purpose Internet policing law, the two groups said in their amicus briefs. The law was passed to criminalize computer hacking in the days of mainframes, before public computer networks really existed. Yet the 9th Circuit's definition of an unauthorized user has exposed all kinds of people to criminal liability for using borrowed passwords, even with the assent of the password holder.

Cato and the EFF both argued that other appellate courts, notably the 2nd and 4th Circuits, have adopted a more circumscribed view of who is an unauthorized user under the CFAA. They both said in their amicus briefs that it's up to the Supreme Court to look at the big-picture question of which users can be targeted under an old law adapted for unanticipated purposes.

"The court is going to have to deal with this issue sooner or later," said Cato's **Devin Watkins**, principal author of the libertarian group's amicus brief backing Power Ventures' petition for Supreme Court review. "The justices are going to have to decide what the underlying principles of the CFAA are." (Cato, like Judge Chen, based its analysis on trespass law. It analogized Power Ventures to a guest invited to an apartment renter's home. Facebook may own the building, but as long as the apartment renter has allowed Power Ventures into the complex, Power Ventures is not trespassing.)

Unless Congress resolves to rewrite the computer fraud law – which it has so far shown absolutely no inclination to do - the Supreme Court will be the last word on weaponizing the CFAA in the frightening ways Judge Chen hypothesized in the LinkedIn case. It's a tough issue that's not going away.