

LinkedIn Takes the Role of Protector of its Users' Privacy

September 13, 2017 – The TMCA

by Ron Moscona



In a recent case brought in a California court, the professional networking service LinkedIn asserted its right to protect its users' privacy expectations against a third party interloper that claims the right to collect their "public" data. Commercial interests are mixed in this case

together with compliance requirements, highlighting the growing tension between free market values and concerns for privacy in cyberspace.

The case in question was brought by data analysis business hiQ Labs, whose activities involve scraping publicly-available profile data of LinkedIn users and analyzing it for its customers (employers and potential employers). LinkedIn wanted to revoke its permission to hiQ to access its open website (which is accessible without registration or password) in order to enforce its terms of use that prohibit data-scraping activities. LinkedIn also wanted to put in place technical measures to prevent data scraping, citing its members' privacy interests as its reason.

HiQ sought an injunction to prevent LinkedIn from blocking its access to the service which it claimed would put it out of business. It asserted various legal theories in support of its case, including alleged violations of California constitutional free speech principles and California competition law. Both parties recruited high profile U.S. counsel – Donald Verrilli for LinkedIn and Laurence Tribe as an advisor to hiQ.

Among other points, LinkedIn argued that hiQ's operations jeopardized its users' privacy

Related People

- Ron Moscona

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

interests. LinkedIn users often update their profile data or change their privacy settings and – it was argued - would not want third-parties such as hiQ to use their old data without regard to their privacy choices. LinkedIn argued that its own services are designed to respect its users' privacy preferences. It provided some statistics showing that millions of LinkedIn users choose not to notify their contacts when they update their profile – suggesting that the users prefer the change to remain unnoticed (with the old profile data being quietly forgotten).

The court (at this stage only on a temporary injunction application) ruled in favor of hiQ. On the limited evidence presented at the preliminary stage, the court found more merit in hiQ's accusations of anti-competitive behavior on the part of LinkedIn than in the latter's concerns for the users' privacy interest. The court stated in this context that the *“actual privacy interests of LinkedIn users in their public data are at best uncertain”*.

The statement reflects an approach that once information is put in the public domain it is no longer confidential and therefore no longer private. However, this is no longer the approach taken by modern privacy laws in many countries. The court's decision did not reference compliance concerns, but it is fair to assume that LinkedIn's decision to block hiQ was at least influenced by its legal duties. Like many others in the digital space, the networking site is undoubtedly aware of the looming requirements of the General Data Protection Regulation (“GDPR”), the EU's overhaul of its privacy legislation which comes into effect in the middle of 2018. One of the requirements of GDPR concerns the so-called ‘right to be forgotten’, or the right of individuals to require their old data to be erased. Similar rules have been introduced in other countries.

Under GDPR, operators of social networks (in most cases) will have to respect users' requests to erase or update their old data. GDPR will also require the operator to notify third-party recipients of the data of user requests to update, correct, or erase the data, and it would need to maintain corporate policies and technology measures to protect the data against unauthorized access, corruption, or loss.

As a global service, LinkedIn needs to take account of developments in privacy protection around the world. It is not clear yet whether compliance with GDPR will require social network operators to prevent unauthorized data scraping by third parties, nor whether LinkedIn would be under an obligation to notify third parties such as hiQ of requests by its users to update or erase their public profiles. However, it is clear that social network operators will have to assume a greater degree of control over the way data flows through and around its network. They may not be able to stop every third party from scraping or using its users' data, but they will need to demonstrate that they are doing as much as they reasonably can to protect the privacy interests of their users.

The result of the temporary injunction application in the hiQ case is probably not of lasting importance. But privacy concerns will continue to arise as digital technologies take an ever growing significance in everyday life. The digital industry can expect to come under closer scrutiny and regulation requiring companies that collect and use data to pay closer attention to the protection of individuals' privacy interests.

For the full article published on CFO Magazine, see [here](#).